基础代数和CF范畴论

邹开其 编著

大连海事大学出版社

国家自然科学基金资助项目
交通部重点科技资助项目

基础代数和 *CF* 范畴论

邹开其　编著

大连海事大学出版社

图书在版编目(CIP)数据

基础代数和 *CF* 范畴论/邹开其编著 .—大连:大连海事大学出版社,2002.8
ISBN 7-5632-1534-4

Ⅰ.基… Ⅱ.邹… Ⅲ.①代数 ②范畴论-高等学校-教材 Ⅳ.O15

中国版本图书馆 CIP 数据核字(2001)第 095797 号

大连海事大学出版社出版
(大连市凌水桥 邮政编码 116026 电话 4728394 传真 4727996)
(http://www.dmupress.com E-mail:cbs@dmupress.com)
大连海事大学印刷厂印装 大连海事大学出版社发行
2002 年 10 月第 1 版 2002 年 10 月第 1 次印刷
开本:850 mm×1 168 mm 1/32 印张:7.25
字数:182 千 印数:0 001~1 000 册
责任编辑:李雪芳 封面设计:王 艳
定价:25.00 元

前　言

《基础代数和 CF 范畴论》是对笔者多年来教学、科研的总结，是笔者继《CF 代数》一书出版后推出的又一本新作。

本书初稿写于 1986 年，是作为应用数学研究生班的教材而编写的，在 10 多年的教学中，笔者听取了师生们的有益建议，几经重大修改，并作为全国高等院校数学教师研讨班的教材再度付印推出。在吸取近年来国内外数学工作者最新科研成果的基础上，终于成书并奉献给读者。

本书在阐述基础代数一些基本概念(如群、环、域和模等)的基础上，介绍了范畴论的基本概念，并用范畴论的观点来统一论述基础代数的各种结构。

北京师范大学汪培庄教授于 1981 年发表的《模糊集和模糊集的范畴》一文，开创了模糊范畴研究的先河，此后这一研究迅速展开。为了总结他人和笔者近年来的科研和教学成果，本书将经典范畴和近年来蓬勃发展的模糊范畴融为一体，详尽地介绍了 CF 范畴的基本内容。基础代数已有漫长的发展历史，要想在一本书中概括所有的基础代数知识几乎是不可能的。它犹如一座大山，内藏宝物，撰写本书的目的就是要给勇敢者一把钥匙，打开大山之门。至于享受挖宝的快乐，还需要他们有更大的勇气。

本书自成系统，读者仅需线性代数的一些基础知识就完全可以读懂它。因此本书可作为非代数专业的应用数学各专业硕士研究生的教材，也可作为大学数学系高年级学生的选修课教材。本书习题分难、中、易三个档次，有精选来的，也有笔者在近年的科研和教学中悟出来的。

笔者谨以此书献给自己的导师——汪培庄教授，是他将笔者

引进了 Fuzzy 的大门，并给予笔者撰写本书的信心和勇气，尽管他远在美国，但对本书的写作和出版还是给予了很多关心和帮助。同时，笔者感谢大连市学术专著资助出版评审委员会，在关键的时刻资助了本书的出版。笔者还感谢大连海事大学出版社提供了这样一个机会，使本书得以问世，特别感谢责编为本书付出的辛勤劳动。由于笔者水平有限，错误和不妥之处在所难免，衷心希望广大读者给以指正。

作　者

2002 年 4 月于大连大学

目　录

第 1 章　集　合

§1.1　集合和类

集合是近代数学的一个基本概念，它的出现，无疑给近代数学的研究奠定了基础。但是它的不恰当的定义，又给近代数学带来了危机。为此，我们首先给出类的概念。

一些对象的全体叫类，使得对每个给定的对象 x，均可决定 x 是否属于该类。而类 A 叫做一个集合，当且仅当存在另一类 B，使得 $A \in B$。故集合是一种特殊的类，类远比集合大得多，不是集合的类叫本性类，本性类确实存在。为此，我们来看一个饶有趣味的例子。

某村有一理发师，规定这位理发师给且只给该村所有那些不给自己理发的人理发。现在，人们问："那位理发师自己的头发由谁理?"这就是著名的"理发师悖论"。若假定理发师的头发由他自己理，按规定，他只能给那些不给自己理发的人理发，故推出他不能为自己理发；若假定他的头发由别人理，即不给自己理，但按规定这位理发师应该去给自己理发。所以，不管理发师的头发由谁理，都得出矛盾。将这个"理发师悖论"公式化，就是 1902 年英国著名哲学家、数学家罗素(B. Russeu)提出的"罗素悖论"。

设有类 $M = \{x \mid x$ 是集合，且 $x \notin x\}$，这里 M 是一个本性类，若将 M 视为集合，则或 $M \in M$ 或 $M \notin M$。若 $M \in M$，由 M 的定义必推出 $M \notin M$，而若 $M \notin M$，又必推出 $M \in M$，不论哪种

情形，都导致一个不能容许的悖论。

上面的例子提醒我们，在使用集合这一术语时，要回避诸如"一切集合的集合"这类提法，以免重蹈悖论的覆辙。至于公理化集合论，我们暂时回避它，因为在研究集合的运算（例如并、交、补、笛卡儿积等）时，有足够多的公理保证这些运算在集合上进行时，其结果也是一个集合。

设 S 为任一集合，其元素用 $a,b,c,\cdots$ 表示，这些元素本身的性质无关紧要，但需注意 $a\in S$ 与 $a\notin S$ 二者必居且仅居其一。对每个集合 S，由 S 的所有子集合构成的类 $\mathscr{P}(S)$ 也是集合，称 $\mathscr{P}(S)$ 为 S 的幂集合，也记做 2^S。

$$\mathscr{P}(S)\triangleq 2^S=\{A\mid A\subseteq S\}$$

集合 S 的元素个数叫集合 S 的基数，记做 $|S|$。显然，若 S 是有 n 个元素的有限集合，记做 $|S|=n$，则 $|\mathscr{P}(S)|=2^n$。

设 I 是指标的集合，简称标集，可以定义

$$\bigcup_{i\in I}A_i=\{x\mid \exists\, i\in I,\text{使得 } x\in A_i\}$$

$$\bigcap_{i\in I}A_i=\{x\mid \forall\, i\in I,\text{使得 } x\in A_i\}$$

若 I 是一个集合，则有公理保证 $\bigcup_{i\in I}A_i$，$\bigcap_{i\in I}A_i$ 均是一个集合。若 $I=\{1,2,\cdots,n\}$，常写 $\bigcup_{i\in I}A_i=A_1\cup A_2\cup\cdots\cup A_n$，$\bigcap_{i\in I}A_i=A_1\cap A_2\cap\cdots\cap A_n$。若 $A\cap B=\varnothing$，称 A 与 B 是不交的。

集合 A 在 B 中的相对补集定义如下：

$$B-A=\{x\mid x\in B\text{ 且 }x\notin A\}$$

如果将我们的讨论限制在一个范围 U 内（U 称为论域），则

$$U-A\triangleq A'=\{x\mid x\in U\text{ 且 }x\notin A\}$$

容易证明下列一些命题：

$$A\cap\left(\bigcup_{i\in I}B_i\right)=\bigcup_{i\in I}(A\cap B_i)$$

$$A\cup\left(\bigcap_{i\in I}B_i\right)=\bigcap_{i\in I}(A\cup B_i)$$

$$\left(\bigcup_{i\in I}A_i\right)'=\bigcap_{i\in I}A_i'$$

$$(\bigcap_{i\in I}A_i)'=\bigcup_{i\in I}A_i' \qquad \text{(De·Morgan 法则)}$$

$$A\cup B=B\Leftrightarrow A\subset B\Leftrightarrow A\cap B=A$$

习题 1.1

1. 证明：如果 $\forall\alpha\in I$，均有 $B_\alpha\subseteq A$，则 $\bigcup_{\alpha\in I}B_\alpha\subseteq A$；如果 $\forall\alpha\in I$，均有 $B_\alpha\supseteq A$，则 $\bigcap_{\alpha\in I}B_\alpha\supseteq A$。其中 I 是一个非空标集。
2. 设 $A_n=(n,\infty)=\{x\mid x\in\mathbf{R}, n<x<\infty, n=1,2,\cdots\}$，求 $\bigcup_{n=0}^{\infty}A_n$，$\bigcap_{n=0}^{\infty}A_n$。
3. 设 S 是有 n 个元素的有限集合，证明：$|\mathscr{P}(S)|=2^n$。
4. 设论域为 U，I 为任一标集，证明下列命题：

   (ⅰ) $A\cap(\bigcup_{i\in I}B_i)=\bigcup_{i\in I}(A\cap B_i)$；

   (ⅱ) $A\cup(\bigcap_{i\in I}B_i)=\bigcap_{i\in I}(A\cup B_i)$；

   (ⅲ) $(\bigcup_{i\in I}A_i)'=\bigcap_{i\in I}A_i'$；

   (ⅳ) $(\bigcap_{i\in I}A_i)'=\bigcup_{i\in I}A_i'$。
5. 设 $A=\bigcup_{i=1}^{\infty}A_i$，证明：存在 A_i 的子集 B_i，$i=1,2,\cdots$，使 $A=\bigcup_{i=1}^{\infty}B_i$，并且对任意 $i\neq j$，均有 $B_i\cap B_j=\varnothing$。

§1.2 映射

映射是函数概念的推广，也是近代数学的一个重要概念，它将贯穿于本书的始终。

定义 1.2.1 设 S，T 是给定的两个集合，如果有一个法则 α，通过它，对 $\forall s\in S$，$\exists!\ t\in T$，使得 $\alpha(s)=t$，称 α 是 S 到 T 的一个映射，S 叫定义域，T 叫上域(Codomain)。

$$(\bigcap_{i\in I}A_i)' = \bigcup_{i\in I}A_i' \qquad \text{(De·Morgan 法则)}$$

$$A\cup B = B \Leftrightarrow A\subset B \Leftrightarrow A\cap B = A$$

习题 1.1

1. 证明：如果 $\forall \alpha\in I$，均有 $B_\alpha\subseteq A$，则 $\bigcup_{\alpha\in I}B_\alpha\subseteq A$；如果 $\forall \alpha\in I$，均有 $B_\alpha\supseteq A$，则 $\bigcap_{\alpha\in I}B_\alpha\supseteq A$。其中 I 是一个非空标集。
2. 设 $A_n=(n,\infty)=\{x\mid x\in\mathbf{R}, n<x<\infty, n=1,2,\cdots\}$，求 $\bigcup_{n=0}^{\infty}A_n$，$\bigcap_{n=0}^{\infty}A_n$。
3. 设 S 是有 n 个元素的有限集合，证明：$|\mathscr{P}(S)|=2^n$。
4. 设论域为 U，I 为任一标集，证明下列命题：

   (ⅰ) $A\cap(\bigcup_{i\in I}B_i)=\bigcup_{i\in I}(A\cap B_i)$；

   (ⅱ) $A\cup(\bigcap_{i\in I}B_i)=\bigcap_{i\in I}(A\cup B_i)$；

   (ⅲ) $(\bigcup_{i\in I}A_i)'=\bigcap_{i\in I}A_i'$；

   (ⅳ) $(\bigcap_{i\in I}A_i)'=\bigcup_{i\in I}A_i'$。
5. 设 $A=\bigcup_{i=1}^{\infty}A_i$，证明：存在 A_i 的子集 B_i，$i=1,2,\cdots$，使 $A=\bigcup_{i=1}^{\infty}B_i$，并且对任意 $i\neq j$，均有 $B_i\cap B_j=\varnothing$。

§1.2 映射

映射是函数概念的推广，也是近代数学的一个重要概念，它将贯穿于本书的始终。

定义 1.2.1 设 S，T 是给定的两个集合，如果有一个法则 α，通过它，对 $\forall s\in S$，$\exists !\ t\in T$，使得 $\alpha(s)=t$，称 α 是 S 到 T 的一个映射，S 叫定义域，T 叫上域(Codomain)。

定义 1.2.1 是用通用法则定义映射的方法，我们再给出用图像定义映射的方法。

设 S 和 T 是两个给定的集合，称

$$S \times T = \{(s,t) \mid s \in S, t \in T\}$$

为 S 和 T 的笛卡儿积。

定义 1.2.1′[①] 由 S 到 T 的一个映射 α 是 $S \times T$ 的一个子集，满足：

(1) $\forall s \in S, \exists t \in T$，使得 $(s,t) \in \alpha$；

(2)若 $(s,t),(s,t') \in \alpha$，则 $t = t'$。

此时，将 S 在 α 下的像记为 $\alpha(S)$。

显然，定义 1.2.1 和定义 1.2.1′是等价的，后者更加直观，我们将经常使用它。

两个映射相等当且仅当它们有相同的定义域、相同的上域和相同的图像。

S 到 T 的映射的集合记为 T^S，

$$T^S = \{\alpha \mid \alpha : S \to T\}$$

设 $A \subseteq S$，称 $\alpha(A) = \{\alpha(a) \mid a \in A\}$ 为 A 在 α 下的像。特别地，$\alpha(S)$ 叫映射的像，记做 $\mathrm{im}\,\alpha$。若把定义域限制在 S 的子集 A 上，则得到一个 A 到 T 的映射，即

$$\beta = \{(a, \alpha(a) \mid a \in A\} \subseteq A \times T$$

称 β 为 α 在 A 上的限制，记做 $\beta = \alpha \mid A$。反之，称 α 是 β 的扩张。

请看一个几何实例(图 1-1)：直线 S 和 T 分别是定义域和上域，O 点是既不在 S 上又不在 T 上的一个固定点，将 S 上的任一点 P 映射到 OP 与 T 的交点 P'，显然，这是一个映射，在射影几何中，称为透视。按定义 1.2.1′，这个映射由 S，T 以及 $S \times T$ 的一

---

① Jacobson N. Basic algebra(Second edition). New York: W. H. Freeman and Company, 1985

个子集 $\alpha=\{(P,P')\mid P\in S,P'\in T\}$ 构成。

当 $\mathrm{im}\,\alpha=T$ 时，称 α 为满射，此时上域 T 即为通常说的值域。若 $s_1\neq s_2\Rightarrow\alpha(s_1)\neq\alpha(s_2)$，称 α 为单射。若 α 既是单射，又是满射，则称 α 为双射。

设 $\alpha:S\to T,\beta:T\to U$，则 α 与 β 的合成映射定义为 $\beta\alpha:S\to U$。$\beta\alpha$ 具有定义域 S，上域 U，且

$$\beta\alpha=\{(s,\beta(\alpha(s)))\mid s\in S\}\subseteq S\times U$$

故 $\beta\alpha(s)=\beta(\alpha(s))$，它可用下面的三角形图形（图 1-2）可换来表示，其中，$\gamma=\beta\alpha$。

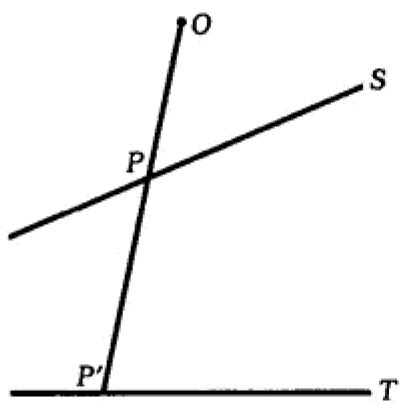


图 1-1

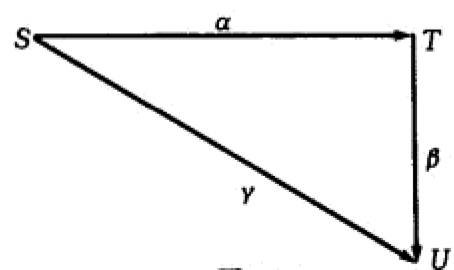


图 1-2

类似地，也有四边形图形可换法则。

设 $\alpha:S\to T,\beta:T\to U,\gamma=S\to V,\delta:V\to U$，则 $\beta\alpha=\delta\gamma$ 可用图 1-3 表示。

映射的合成满足结合律，设 $\alpha:S\to T,\beta:T\to U,\gamma:U\to V$，则

$$\gamma(\beta\alpha)=(\gamma\beta)\alpha$$

证明是容易的，仅用示意图（图 1-4）说明。

映射的结合律说明，只要 $\triangle STU$ 和 $\triangle TUV$ 可换，则整个图形可换。

对任意集合 S，定义恒等映射 $1_S:S\to S$，其中

$$1_S = \{(s,s) \mid s \in S\}$$

称 1_S 为 S 的对角线,在不混淆的前提下,也可简记为 1。

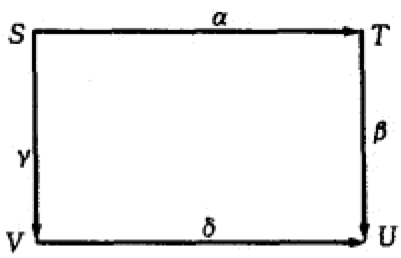


图 1-3

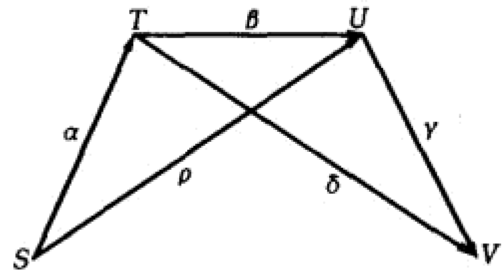


图 1-4

显然有 $1_T\alpha = \alpha 1_S$,下面给出重要命题。

命题 1.2.1 $\alpha: S \to T$ 是双射当且仅当 $\exists \beta: T \to S$,使得 $\beta\alpha = 1_S$ 及 $\alpha\beta = 1_T$。

证 必要性 $\forall s \in S$,由 $\alpha(s) \in T$,故 $\beta = \{(\alpha(s), s) \mid s \in S\} \subseteq T \times S$。对 $\forall t \in T$,因 α 是满射,故 $\exists s \in S$,使得 $\alpha(s) = t$,又 α 是单射,若 $(t, s_1), (t, s_2) \in \beta$,则 $\alpha(s_1) = t = \alpha(s_2) \Rightarrow s_1 = s_2$,故 β 是映射。

又 $\forall s \in S$,由 $(s, \alpha(s)) \in \alpha$ 和 $(\alpha(s), s) \in \beta$ 得

$$\beta\alpha(s) = \beta(\alpha(s)) = s$$

故 $\beta\alpha = 1_S$。同理可证 $\alpha\beta = 1_T$。

充分性 $\forall t \in T$,则 $\beta(t) = s \in S$,故 $\alpha(s) = \alpha(\beta(t)) = \alpha\beta(t) = 1_T(t) = t$,故 α 是满射。

若 $\alpha(s_1) = \alpha(s_2)$,则 $s_1 = \beta(\alpha(s_1)) = \beta(\alpha(s_2)) = s_2$,故 α 是单射。

由此完成了命题的证明。

显然,满足 $\beta\alpha = 1_S$ 和 $\alpha\beta = 1_T$ 的 β 是惟一的,把这个 β 记做 α^{-1},有 $(\alpha^{-1})^{-1} = \alpha$。

命题 1.2.2 两个双射的积是双射,即设 $\alpha: S \to T$, $\beta: T \to U$ 都是双射,则 $\beta\alpha$ 也是双射,且

$$(\beta\alpha)^{-1} = \alpha^{-1}\beta^{-1}$$

证 显然有 $\alpha^{-1}: T \to S, \beta^{-1}: U \to T$,且

$$\alpha^{-1}\beta^{-1}: U \to S$$

$$(\beta\alpha)(\alpha^{-1}\beta^{-1}) = \beta(\alpha\alpha^{-1})\beta^{-1} = \beta\beta^{-1} = 1_U$$

$$(\alpha^{-1}\beta^{-1})(\beta\alpha) = \alpha^{-1}(\beta^{-1}\beta)\alpha = \alpha^{-1}\alpha = 1_S$$

故 $(\beta\alpha)^{-1} = \alpha^{-1}\beta^{-1}$。

公式 $(\beta\alpha)^{-1} = \alpha^{-1}\beta^{-1}$ 称为穿脱原理,犹如在穿脱鞋、袜时,脱时按穿时的相反顺序进行。

本节最后指出,笛卡儿积的概念可以推广到任意有限多个集合。

设 $S_1, S_2, \cdots, S_n$ 是任意 n 个集合,则称

$$\prod_{i=1}^{n} S_i \triangleq S_1 \times S_2 \times \cdots \times S_n = \{(s_1, s_2, \cdots, s_n) \mid s_i \in S_i, i = 1, 2, \cdots, n\}$$

为 n 个集合 $S_1, S_2, \cdots, S_n$ 的笛卡儿积。

此概念也可推广到任意无限多个集合,设 I 是任一指标集,

$$\prod_{i \in I} S_i = \{\alpha \mid \alpha: I \to \bigcup_{i \in I} S_i, \alpha(i) \in S_i, \forall i \in I\}$$

习题 1.2

1. 设 $f: A \to B, g: B \to C$,证明:

   (i)若 f, g 都是单射,则 gf 也是单射;

   (ii)若 f, g 都是满射,则 gf 也是满射。

2. 称 φ_2 是 $\varphi_1: U \to V$ 的左逆映射,当 $\varphi_2: V \to U$,且 $\varphi_2\varphi_1 = 1_U$ 时。设 $f: A \to B, g: B \to C$,且 gf 有左逆映射,能否证明 f, g 都有左逆映射?

3. 对于下面给出的 $\mathbf{Z}$ 到 $\mathbf{Z}$ 的映射 f, g, h, $\forall x \in \mathbf{Z}$, $f(x) = 3x$, $g(x) = 3x + 1$, $h(x) = 3x + 2$,请:

(ⅰ)分别求出它们的左逆映射；

(ⅱ)找出 f,g,h 共同的左逆映射，即找出 $\mathbf{Z}$ 到 $\mathbf{Z}$ 的映射 k，使 $kf=kg=kh=1_{\mathbf{Z}}$。

(ⅲ)找一个 $\mathbf{Z}$ 到 $\mathbf{Z}$ 的映射，使其为 f,g 的共同的左逆映射，但不是 h 的左逆映射。

4. 找出 $\mathbf{Z}$ 到 $\mathbf{Z}$ 的 $n+1$ 个映射 $f_i, i=1,2,\cdots,n+1$，使 $f_1,f_2,\cdots,f_n$ 有共同的左逆映射 g，但 g 不是 f_{n+1} 的左逆映射。

5. 设 A,B,C 是集合 E 的 3 个子集，且 $A=B\cup C, B\cap C=\varnothing$，找出 2^A 到 $2^B\times 2^C$ 的一个双射。

6. 证明：不存在 A 到 2^A 的双射，此处 $A\neq\varnothing$。

7. 设 $S=\{1,2,\cdots\}$，试给出 S 到 S 的两个映射 α,β 的实例，使得 $\alpha\beta=1_S$，但 $\beta\alpha\neq 1_S$；如果 α 是双射，这是否有可能？

8. 证明，$\alpha: S\to T$ 是单射当且仅当存在映射 $\beta: T\to S$，使得 $\beta\alpha=1_S$；α 是满射当且仅当存在映射 $\beta: T\to S$，使 $\alpha\beta=1_T$。在这两种情况下，判断下述断言是否成立：如果 β 是惟一的，则 α 是双射。

9. 证明，$\alpha: S\to T$ 是满射的充要条件是不存在 T 到集合 U 的映射 β_1,β_2，使得 $\beta_1\neq\beta_2$，但 $\beta_1\alpha=\beta_2\alpha$；$\alpha$ 是单射的充要条件是不存在集合 U 到 S 的映射 γ_1,γ_2，使得 $\gamma_1\neq\gamma_2$，$\alpha\gamma_1=\alpha\gamma_2$。

10. 设 $\alpha: S\to T$，A 和 B 是 S 的子集，证明：$\alpha(A\cup B)=\alpha(A)\cup\alpha(B)$ 和 $\alpha(A\cap B)\subset\alpha(A)\cap\alpha(B)$，举例说明 $\alpha(A\cap B)$ 不一定和 $\alpha(A)\cap\alpha(B)$ 重合。

11. 设 $\alpha: S\to T$，A 是 S 的子集，A' 是 A 在 S 中的补集，证明：一般情况下，$\alpha(A')\not\subset(\alpha(A))'$，$(\alpha(A))'$ 是 $\alpha(A)$ 在 T 中的补集，如果 α 是单射，情形如何？如果 α 是满射，情形如何？

§1.3 等价关系

将映射的定义放宽，可得关系的定义，它仅仅要求是笛卡儿积的一个子集，而放宽了对定义 1.2.1′中(2)的限制，故关系是映射概念的推广。这里，我们仅研究集合 S 上的二元关系。

定义 1.3.1 集合 S 上的一个二元关系 R 是 $S\times S$ 的一个子集合，若 $(a,b)\in R$，则说 a 与 b 有关系 R，记为 aRb。

定义 1.3.2 集合 S 上的一个二元关系 E 叫等价关系，如果：

(1) $\forall a\in S, aEa$ （反身性）；

(2) $\forall a,b\in S$，若 aEb，则 bEa （对称性）；

(3) $\forall a,b,c\in S$，若 aEb,bEc，则 aEc （传递性）。

S 上的任一等价关系都可确定一个分类，反之，S 的任一分类都可确定 S 的一个等价关系。

例如：设 E 是 S 的一个等价关系，设 $a\in S$，令

$$\bar{a} = \{b \mid b \in S, bEa\}$$

容易证明：$\bigcup\limits_{a\in S}\bar{a}=S$，且对 $\forall a,b\in S$，或 $\bar{a}=\bar{b}$ 或 $\bar{a}\cap\bar{b}=\varnothing$。

称由 E 决定的一个分类 $\pi=\{\bar{a}\mid a\in S\}$ 为 S 对于 E 的商集，记做 S/E。令

$$\gamma: S\rightarrow S/E$$
$$a\rightarrow\bar{a}$$

则称 γ 是 S 到商集合 S/E 的自然映射，显然，γ 是满射。

下面我们通过等价关系来对一个映射进行分解，这对后面的研究是至关重要的。

设 α 是 S 到 T 的一个映射，在 S 里定义关系 E_α：$aE_\alpha b\Leftrightarrow \alpha(a)=\alpha(b)$，显然，这是一个等价关系。设 $c\in T$，c 的原像为

$$\alpha^{-1}(c) = \{a \mid a \in S, \alpha(a) = c\}$$

而当 $c\notin \mathrm{im}\,\alpha$ 时，$\alpha^{-1}(c)=\varnothing$。

设 $C\subseteq T$，C 的原像为

$$\alpha^{-1}(C)=\{a\in S\mid \alpha(a)\in C\}=\bigcup_{c\in C}\alpha^{-1}(c)$$

另一方面，若对 $a\in S$，有 $c=\alpha(a)$，则

$$\alpha^{-1}(c)=\alpha^{-1}(\alpha(a))=\{b\mid \alpha(b)=\alpha(a)\}$$

这恰是 S 中由 a 确定的等价类 $\bar{a}_{E_\alpha}$，称之为 c 上的纤维(fiber)，这种纤维的集合 $\{\alpha^{-1}(c)\mid c\in \mathrm{im}\,\alpha\}$ 构成了 S 的一个分类，从而决定 S 的一个等价关系，利用这个等价关系，可将映射 α 进行分解。

定理 1.3.1 设 $\alpha:S\to T$，则 α 可确定 S 的一个分类，并且存在惟一的 $\bar{\alpha}:S/E_\alpha\to T$，使得 $\alpha=\bar{\alpha}\gamma$，其中 γ 为自然映射，且 α 是满射的充分必要条件是 $\bar{\alpha}$ 是双射。

证 上面由 α 确定的 S 的分类为 $\pi=\{\bar{a}_{E_\alpha}\mid a\in S\}$，令

$$\bar{a}_{E_\alpha}=\alpha^{-1}(\alpha(a))\triangleq\bar{a}$$

定义

$$\bar{\alpha}:S/E_\alpha\to T$$
$$\bar{a}\ \to\alpha(a)$$

由 $\bar{a}=\bar{b}\Rightarrow\alpha(a)=\alpha(b)$，故 $\bar{\alpha}$ 与代表元选择无关，$\bar{\alpha}$ 确为映射，又由 $\alpha(a)=\alpha(b)\Rightarrow\bar{a}=\bar{b}$，故 $\bar{\alpha}$ 是单射。显然有 $\bar{\alpha}(\gamma(a))=\bar{\alpha}(\bar{a})=\alpha(a)$，故 $\alpha=\bar{\alpha}\gamma$。而因 γ 是满射，故 $\mathrm{im}\,\alpha=\mathrm{im}\,\bar{\alpha}$，因此 $\bar{\alpha}$ 是双射当且仅当 α 是满射。

最后证明这样的 $\bar{\alpha}$ 是惟一的，即若存在

$$\beta:S/E_\alpha\to T$$

使得 $\beta\gamma=\alpha$，则 $\beta(\bar{a})=\beta(\gamma(a))=\alpha(a)=\bar{\alpha}(\bar{a})$，故 $\beta=\bar{\alpha}$。

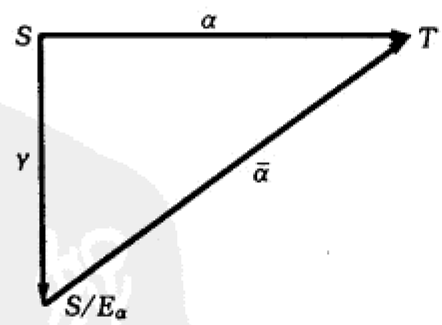


图 1-5

映射的分解可由图 1-5 示意。

若给定映射 $\alpha:S\to T$，S 上的一个等价关系 E，注意，这里的

E 不一定是由 α 决定的，但却与 α 相容，即 $\forall a,b\in S$，由 $aEb\Rightarrow\alpha(a)=\alpha(b)$，此时，仍有映射的分解定理。

定理 1.3.2 设 $S\rightarrow T$，E 是 S 的一个等价关系，且 α 和 E 相容，则存在惟一的满射 $\bar{\alpha}:S/E\rightarrow T$，使得

$$\alpha=\bar{\alpha}\gamma$$

且 $\bar{\alpha}$ 是单射当且仅当 $E=E_\alpha$。

证明是容易的，留给读者。

习题 1.3

1. $(F)_n$ 表示数域 F 上全部 n 阶方阵的集合，f 是 $(F)_n$ 到 $\{0,1,2,\cdots,n\}$ 上的满射

$$f:(a_{ij})\rightarrow 秩(a_{ij})$$

求 f 决定的等价关系、等价类。

2. 设 R_1,R_2 是 A 的两个等价关系，$R_1\cap R_2$ 是不是 A 的二元关系？是不是等价关系？为什么？$R_1\cup R_2$ 是不是 A 的二元关系？是不是等价关系？为什么？

3. 设 R 为 A 的一个二元关系，证明：存在惟一的包含 R 的最小等价关系。

4. $f:S\times S\rightarrow S$ 称为集合 S 上的一个二元运算。设 R_1,R_2 是 A 的两个二元关系，规定

$$R_1\circ R_2=\{(a,b)\mid\exists x\in A,(a,x)\in R_1,(x,b)\in R_2\}$$

证明：$\circ$ 是 A 的一切二元关系所构成的集合 B 上的一个二元运算。

5. 证明，S 上的一个关系 E 是等价关系的条件是：

(i) $E\supset 1_S$；

(ii) $E=E^{-1}$；

(ⅲ)$E \supset EE$。

6. 设 C 为 S 上的二元关系，对 $r=1,2,3,\cdots$，定义 $C^r=\{(s,t) \mid$ 对某些 $s_1,s_2,\cdots,s_{r-1}\in S$，有 $sCs_1,s_1Cs_2,\cdots,s_{r-1}Ct\}$，令

$$E=1_S\cup(C\cup C^{-1})\cup(C\cup C^{-1})^2\cup(C\cup C^{-1})^3\cup\cdots$$

证明：E 是一个等价关系，而且 S 上的每个含有 C 的等价关系都包含 E，E 叫做由 C 生成的等价关系。

7. 元素的个数分别为 2,3,n 的集合 S 上，各有多少个不同的二元关系？各有多少个不同的等价关系？

§1.4 数学归纳法

在许多数学问题的证明中，经常使用数学归纳法，我们将从自然数系 0,1,2,…出发，来研究应用数学归纳法原理证明命题的根据。

首先给出自然数系的一个公理，即传统的 Peano 公理。

Peano 公理 设 N 是一个非空集合，N 中有一个初始元素，记做 0，存在后继映射

$$\varphi: N\to N$$
$$a\to a^+$$

满足：

(1) $\forall a\in N, a^+\neq 0$；

(2) φ 是单射；

(3) N 的任一含有 0 的子集，如果含有这个子集中每个元素的后继元，则它与 N 重合。

从 Peano 公理可直接推出第一归纳法。

定理 1.4.1 （第一归纳法）

设有一个与自然数有关的命题 $E(n)$，如果 $E(0)$ 是真的，且若 $E(r)$ 为真，则 $E(r^+)$ 也为真，则对 $\forall n\in\mathbf{N}$，$\mathbf{N}$ 为自然数集合，

$E(n)$是真的。

证 令 $S=\{s \mid E(s)$是真的$\}$,则 $0\in S$,且当 $r\in S$ 时,$r^+\in S$。由 Peano 公理(3),得 $S=\mathbf{N}$,故对 $\forall n\in\mathbf{N}$,$E(n)$是真的。

由归纳法可以证明命题,用归纳法也可以定义概念,这首先需要下面的逆归定理。

定理 1.4.2 (逆归定理)

设 S 为一集合,$\varphi: S\to S$,取 $a\in S$,则存在惟一的映射 $f:\mathbf{N}\to S$,使得

(1) $f(0)=a$;

(2) $f(n^+)=\varphi(f(n))$, $\forall n\in\mathbf{N}$。

证 考虑笛卡儿积 $\mathbf{N}\times S$,令 $\Gamma=\{U \mid U\subset\mathbf{N}\times S, (0,a)\in U$,且若$(n,b)\in U$,则$(n^+,\varphi(b))\in U, n\in\mathbf{N}, b\in S\}$,显然 $\mathbf{N}\times S\in\Gamma$,故 $\Gamma\neq\varnothing$,设 $f=\bigcap\limits_{U\in\Gamma}U$,显然,$f\in\Gamma$,往证 f 即为所要证之映射。

首先,由归纳法易证:$\forall n\in\mathbf{N}$, $\exists b\in S$,使得$(n,b)\in f$。其次,令

$$T=\{n\in\mathbf{N} \mid (n,b),(n,b')\in f\Rightarrow b=b'\}$$

① $0\in T$,因若不然,$(0,a),(0,a')\in f$,但 $a\neq a'$,令 $f'=f\setminus(0,a')\subsetneq f$,而 $f'\in\Gamma$(f'为 f 中去掉$(0,a')$,但 $n^+\neq 0$),故 $f'\supset f$,此为矛盾。

②若 $r\in\mathbf{N}$ 且 $r\in T$,但 $r^+\notin T$,令$(r,b)\in f$,则$(r^+,\varphi(b))\in f$,而 $r^+\notin T$,由 T 的定义,$\exists c\neq\varphi(b)$,使得$(r^+,c)\in f$。令 $f'=f\setminus(r^+,c)\subsetneq f$,因 $r^+\neq 0$,而$(0,a)\in f\Rightarrow(0,a)\in f'$,同样,若 $n\in\mathbf{N}$, $n\neq r$, $(n,d)\in f'$,则$(n^+,\varphi(d))\in f'$(后继映射是单射)。现设$(r,b')\in f'$,则 $b=b'$,而 $\varphi(b)\neq c$,故$(r^+,\varphi(b))\neq(r^+,c)\Rightarrow(r^+,\varphi(b))\in f'\Rightarrow f'\in\Gamma$。故 $f'\supset f$ 与 $f'\subsetneq f$ 矛盾。此矛盾说明,若 $r\in T$,则 $r^+\in T$。

由归纳法,$T=\mathbf{N}$,f 的存在性证完。

再证 f 的惟一性：设 g 是任一满足条件的映射，则 $g\in\Gamma\Rightarrow g\supset f$，由映射定义 $g=f$。

自然数系还具有一个重要性质——良序性。

定理 1.4.3 在 $\mathbf{N}$ 的任意非空子集 S 中，存在最小数，即存在 $l\in S$，使得 $\forall s\in S$，有 $l\leqslant s$。

证 令 $M=\{m\in\mathbf{N}\mid m\leqslant s,\forall s\in S\}$，则 $0\in M$，若 $s\in S$，则 $s^+\notin M$，故 $M\neq\mathbf{N}$。由归纳法，$\exists l\in M$，但 $l^+\notin M$，则 l 即为 S 的最小数，这是因为 $\forall s\in S$，有 $l\leqslant s$，且 $l\in S$，若不然，$\forall s\in S$，有 $l<s\Rightarrow l^+\leqslant s$，与 $l^+\notin M$ 矛盾。

由良序性可以导出第二归纳法。

第二归纳法 设 $E(n)$是与自然数 n 有关的命题，若对所有的 $s<r$，$E(s)$为真，证得 $E(r)$也为真，则 $\forall n\in\mathbf{N}$，$E(n)$是真的。

证 令 $F=\{r\in\mathbf{N}\mid E(r)\text{不真}\}$，若 $F\neq\varnothing$，则 F 含有最小数 l，$F(l)$不真，但对每个 $s<l$，$F(s)$都是真的，由条件推得 $F(l)$为真，此为矛盾，故 $F=\varnothing$，即对 $\forall n\in\mathbf{N}$，$E(n)$是真的。

§1.5 超限归纳法

本节首先建立集合的序关系。

设 S 是一个集合，S 上的二元关系“$\leqslant$”如果满足

(1) $\forall a\in S,a\leqslant a$；

(2) $\forall a,b\in S,a\leqslant b$ 且 $b\leqslant a\Rightarrow a=b$；

(3) $\forall a,b,c\in S,a\leqslant b$ 且 $b\leqslant c\Rightarrow a\leqslant c$。

称“$\leqslant$”为 S 的一个偏序，将$(S,\leqslant)$称为偏序集。

显然，在偏序集中，并非任意元素都可比较，即 $\forall a,b\in S$，未必有 $a\leqslant b$ 或 $b\leqslant a$，若偏序集$(S,\leqslant)$中任两个元素均可比较，则称“$\leqslant$”为全序(线性序)，相应地，$(S,\leqslant)$称为全序集(线性序集)。

设$(S,\leqslant)$为偏序集，元素 $a\in S$ 叫做 S 中的一个极大元是指

$\forall b \in S$,若 $a \leqslant b \Rightarrow a = b$,换句话说,$S$ 中设有比 a 更大的元,若有的话,就是它本身。注意极大元并非最大元,一个给定的偏序集可能有若干个极大元,也可能无极大元,对极小元同样可以定义。

S 的一个非空子集 A 的上界是指 $\alpha \in S$,且对 $\forall a \in A$,有 $a \leqslant \alpha$,注意上界不一定惟一,且 A 的上界不一定在 A 中,A 可能有若干个上界,这些上界中最小的称为最小上界,同样可以定义下界和最大下界。

下面介绍 Zorn 引理。可以证明 Zorn 引理等价于选择公理,因此我们视它为公理,以便引用。

Zorn 引理 设$(S,\leqslant)$是一个非空的偏序集,则它的任一非空全序子集有上界。

将自然数系的良序性加以推广,可得良序集的定义。

设 A 是偏序集$(S,\leqslant)$的非空子集,元素 $c \in A$ 叫 A 的最小元,是指 $\forall a \in A \Rightarrow c \leqslant a$。如果 S 的每个非空子集均有最小元,则称 S 为良序集。

每个良序集均为全序集,这是因为 $\forall a, b \in S$,$\{a, b\}$ 均有最小元,即或者 $a \leqslant b$ 或者 $b \leqslant a$,反之不一定。但由 Zorn 引理可以证明,对 S 规定适当的序关系,可以使之成为良序集,即任意集合均可良序化。

利用良序集的概念,可以得到超限归纳法。

定理 1.5.1 (超限归纳法)

设$(S,\leqslant)$是一个良序集,$p(x)$是与 $x \in S$ 有关的一个命题,如果

(1)对 S 中的最小元 c,$p(c)$为真;

(2)设 $\forall x < a$,$p(x)$为真,可以推出 $p(a)$为真。

则对 $\forall x \in S$,$p(x)$均为真。

证 设 $W = \{x \in S \mid p(x)\text{不真}\}$,若 $W \neq \varnothing$,则 W 有最小元 b,$b \neq c$,由(1)知 $c \notin W$;另一方面,b 是 W 中的最小元,故 $\forall x <$

b，$p(x)$为真，但由(2)知 $p(b)$为真，此为矛盾，故 $W=\varnothing$，即对 $\forall x\in S$，$p(x)$均为真。

习题 1.4

1. 证明，第一归纳法可推广为：如果 $s\in \mathbf{N}$，且对每个 $n\geqslant s$ 有命题 $E(n)$，假设 $E(s)$是真的，并且由 $E(r)$对 $r\geqslant s$ 真，能推得 $E(r^{+})$真，则 $E(n)$对所有的 $n\geqslant s$ 是真的。叙述并证明第二归纳法原理的类似推广。
2. 用归纳法证明：如果 c 为大于等于 -1 的实数，$n\in \mathbf{N}$，则
$$(1+c)n\geqslant 1+nc$$
3. 设 $N=\{0,1\}$，且规定 $0^{+}=1,1^{+}=1$，证明：N 满足 Peano 公理(1)和(3)，但不满足(2)。
4. 举一个有序集$(S,\leqslant)$但不是良序集的例子，并对 S 规定另一种偏序关系，使之成为良序集。
5. 证明：有限偏序集的每一非空子集均有极小元。
6. 证明：设$(A,\leqslant)$是偏序集，T 是$(2^{A},\subseteq)$的一个子集，命 $\bar{T}=\{y\mid y\in 2^{A},y\subseteq t,t\in T\}$，则 T 与 $\bar{T}$ 有相同的极大元。
7. 证明：设$(S,\leqslant)$是有序集，则$(S,\leqslant)$是良序集的充要条件是对任意 $a\in S$，$Sa=\{x\mid x\in S,x<a\}$是良序集。
8. 证明：设$(S,\leqslant)$是偏序集，如果 S 中每一非空子集 M 均有极大元，那么 S 中任一递增序列 $a_1<a_2<\cdots<a_n<\cdots$ 必终止于有限项，反之亦然。

第2章　群

群论是代数中最古老最丰富的分支,群论中若干专门深刻的结果,本书不去讨论它,本章仅研究群的一些最基本的概念和结论。

由于近代数学的一些新的分支,如自动机理论、模糊数学等极大地促进了半群的研究,使半群理论日趋丰富,本章将从含有单位元的半群——亚群开始,但仅仅介绍一些概念,而不做深入的研究。

§2.1　亚群和群

在第1章已经谈到,集合映射的合成满足结合律,特别称 S 到自身的映射为变换,S 的所有变换的集合记为 $M(S)$,显然,若 $|S|=n$,则 $|M(S)|=n^n$。

设 M 是一个非空集合,称

$$p:M\times M\rightarrow M$$

为 M 的一个二元运算。

显然,$M(S)$有一个二元运算即变换的合成,且含有一个恒等变换 $1_{M(S)}$,称这个代数结构为变换亚群。

定义 2.1.1　设 M 是非空集合,p 是 M 中可结合的二元运算,且 $1\in M$,$\forall a\in M$,有 $p(1,a)=a=p(a,1)$,称$(M,p,1)$为亚群。

在定义 2.1.1 中,若去掉关于 1 的假设,称(M,p)为半群。显然,亚群是含 1 的半群,称 1 为 M 的单位元。设 $1'$是另一个单

位元，则 $1'1=1=1'$，故单位元是惟一的。

例 1 (N, + ,0)是亚群，其中 N 是自然数集，+ 是通常的加法，0 是 N 中的零元。

例 2 (N,·,1)是亚群，其中"·"是通常乘法，1 是自然数 1。

例 3 (Z, + ,0)，(Z,·,1)均是亚群。

例 4 设 S 是任意非空集合，则$(\mathscr{P}(S),\cup,\varnothing)$与$(\mathscr{P}(S),\cap,S)$均是亚群。

由以上几例可以看出，二元运算的定义相当广泛，远远超出了通常运算的含义，通常将 $p(a,b)\triangleq ab$。

定义 2.1.2 设 M 是亚群，$N\subset M$，若 $1\in N$，且在 N 中乘法封闭，即 $\forall n_1,n_2\in N\Rightarrow n_1n_2\in N$，则 N 叫做 M 的子亚群，N 是 M 的子亚群简记为 $N\leqslant M$。

一个亚群如果有有限个元素，称这个亚群为有限亚群，否则称为无限亚群，亚群 M 的基数叫 M 的阶，记做 $|M|$。

设 u 为亚群 M 的元素，如果 $\exists v\in M$，使得

$$uv = vu = 1$$

则 u 叫可逆元，v 叫做 u 的逆元。

设 v' 也满足 $uv'=v'u=1$，则 $v'=(vu)v'=v(uv')=v$，故逆元是惟一的，记做 $v=u^{-1}$，显然，u^{-1} 也是可逆元，且

$$(u^{-1})^{-1} = u$$

定义 2.1.3 一个亚群$(G,p,1)$，如果 G 中所有元素都是可逆元，则称做群。

亚群 M 的子亚群 N 如果是群，则称 N 是 M 的子群。

定义 2.1.4 亚群 M 的子集 G 是子群，当且仅当 G 具有性质：

(1) $1\in G$；

(2) $\forall g_1,g_2\in G$，有 $g_1g_2\in G$；

(3) $\forall g\in G$，有 $g^{-1}\in G$。

显然，亚群 M 中的元素不一定都是可逆元，但若将 M 中的所有可逆元收集在一起，记为 $U(M)$，则 $U(M)$是 M 的子群，我们称之为 M 的可逆元群。

例如，$M(S)$的可逆元群 $U(M(S))$是 S 的双射变换的集合，称$(U(M(S)),p,1)$为集合 S 的对称群，记为 Sym S。特别地，若 $S=\{1,2,\cdots,n\}$，则把 Sym S 记为 S_n，通常把 S_n 的元素叫$\{1,2,\cdots,n\}$的置换，故也称 S_n 为置换群，可以验证$|S_n|=n!$。

请看群的一些例子。

例 5 $(\mathbf{Z},+,0)$整数加法群，其中 a 的逆元是 $-a$；类似地，$(\mathbf{Q},+,0)$是有理数加法群，$(\mathbf{R},+,0)$是实数加法群，$(\mathbf{C},+,0)$是复数加法群。

例 6 $(\mathbf{Q}^*,\cdot,1)$是非零有理数乘法群，a 的逆元 a^{-1} 即为通常的倒数$\frac{1}{a}$。类似地$(\mathbf{R}^*,\cdot,1)$是非零实数乘法群，$(\mathbf{C}^*,\cdot,1)$是非零复数乘法群。

例 7 平面绕原点 O 的旋转的集合，合成为通常的旋转合成，则旋转角为 θ 的旋转 α 可表示为映射$(x,y)\to(x',y')$，其中

$$x' = x\cos\theta - y\sin\theta$$
$$y' = x\sin\theta + y\cos\theta$$

当 $\theta=0$ 时，得恒等变换，而 α^{-1}是以 $-\theta$ 为旋转角的旋转。

例 8 例 7 中的集合再并以关于通过原点 O 的直线的反射的集合，反射 $\beta:(x,y)\to(x',y')$，其中

$$x' = x\cos\theta + y\sin\theta$$
$$y' = x\sin\theta - y\cos\theta$$

易证两个反射的积是旋转，而一个反射与一个旋转按随便哪一个顺序的积都是反射。

例 9 设 $D_n=\{$将正 n 边形映射为自身的旋转和反射$\}$，显然，旋转皆为对称旋转，共有 n 个，记为 $R_1,R_2,\cdots,R_n$。设 S 为

关于 x 轴的反射，T 为任意反射对称，则

$$ST = R_i, i = 1,2,\cdots,n$$

又 $S^2=1$，故 $S(ST)=SR_i \Rightarrow T=SR_i$。

故用 n 个对称旋转右乘关于 x 轴的反射对称，得到全部的反射对称，共有 n 个，因此 $|D_n|=2n$，称群 D_n 为二面体群。

例 10 令 $U_n=\{z\in\mathbf{C} \mid z^n=1\}$，则容易验证 $(U_n,\cdot,1)$ 是一个群，称为 n 次单位根群，它是 $(\mathbf{C},\cdot,1)$ 的子群，简记为 $U_n\leqslant\mathbf{C}$。

例 11 由已知的群可以构造一个新的群。例如，设 $G_1,G_2,\cdots,G_n$ 是群，令

$$\prod_{i=1}^{n} G_i \triangleq G_1\times G_2\times\cdots\times G_n =$$
$$\{(a_1,a_2,\cdots,a_n) \mid a_i\in G_i, i=1,2,\cdots,n\}$$

在 $\prod\limits_{i=1}^{n} G_i$ 中定义乘法

$$(a_1,a_2,\cdots,a_n)\cdot(b_1,b_2,\cdots,b_n) =$$
$$(a_1b_1,a_2b_2,\cdots,a_nb_n),\quad a_i,b_i\in G_i$$

取 $1=(1_1,1_2,\cdots,1_n)$，1_i 是 G_i 的单位元，$i=1,2,\cdots,n$，容易验证 $(\prod\limits_{i=1}^{n} G_i,\cdot,1)$ 是群，称为群 $G_1,G_2,\cdots,G_n$ 的直积群。

例 12 设 S_n 是 n 次置换群，$\forall\alpha\in S_n$，由高等代数知 α 可表为不相交的循环的积，而每一循环又可表为若干对换之积，故 α 可表为若干对换之积。若对换个数为偶数个，则称为偶置换；若对换个数为奇数个，则称为奇置换。令

$$A_n = \{\beta \mid \beta\in S_n, \beta\text{ 是偶置换}\}$$

易证 A_n 是 S_n 的子群，称 A_n 为交代群，且 $|A_n|=\dfrac{n!}{2}$。

例 13 设 G 是群，$S\subset G$，令

$$\langle S\rangle=\bigcap\{G_\alpha \mid G_\alpha\leqslant G, \text{且 } G_\alpha\supset S\}$$

显然,$\langle S\rangle$是 G 的子群,因为子群的交还是子群(读者自行验证),且是包含 S 的最小的子群,称之为由 S 生成的子群。

特别地,若 S 是有限集合,即 $S=\{s_1,s_2,\cdots,s_n\}$,则记

$$\langle S\rangle \triangleq \langle s_1,s_2,\cdots,s_n\rangle$$

一般地,记$\langle S\rangle=\{1,s_1s_2\cdots s_r \mid s_i \text{ 或 } s_i^{-1}\in S, i=1,2,\cdots,r\}$。

习题 2.1

1. 设 S 为集合,并以 $ab=b$ 定义 S 里的乘积,证明:
   (i) S 是半群;
   (ii)在什么条件下,S 含有单位元素?
2. 设$(M,p,1)$是亚群,$m\in M$,在 M 中定义一个新乘积 p_m,$p_m(a,b)=amb$,证明:
   (i)这定义了一个半群;
   (ii)在与 m 有关的什么条件下,有关于 p_m 的单位元素?
3. 设 S 是半群,u 为不属于 S 的元素,令 $M=S\cup\{u\}$,对所有 $a\in M$,定义 $ua=a=au$,利用此定义,把 S 里的乘积扩充成 M 里的二元乘积,证明:M 是亚群。
4. 设 S 表示集合 A 的一切二元关系所成集合,证明:S 关于二元关系的合成“$\circ$”构成一个亚群。
5. 证明,半群 G 如果具有下列性质,则成为群:
   (i) G 有一个右单位元 l_r;
   (ii) G 的每个元 a 对于 l_r 有一个右逆元。
6. 设 G 为半群,且对于 G 中任何元素 a 与 b,方程 $ax=b$ 及 $ya=b$ 在 G 中都有解,证明 G 是群。反之,在群 G 中,证明:对任意 $a,b\in G$,$ax=b$ 和 $ya=b$ 在 G 中都有解。
7. 设亚群的元素 a 有右逆元素 b,即 $ab=1$,有左逆元素 c,即

$ca=1$。证明：$b=c$ 且 a 是可逆的，$a^{-1}=b$；再证明 a 是可逆的，且逆元素为 b，必须而且只须 $aba=a$ 及 $ab^2a=1$。

8. 设 G 为亚群 M 的非空子集，证明：G 是子群的充要条件是对 $\forall g\in G$，g 在 M 里是可逆的，且对 $\forall g_1,g_2\in G$，有 $g_1^{-1}g_2\in G$。

9. 证明：

   (ⅰ)在群中双边消去群成立，即 $ax=ay\Rightarrow x=y$；$xa=ya\Rightarrow x=y$。

   (ⅱ)任一使消去律成立的有限半群是群。

10. 称 S 是一个交换半群(群)，若 $\forall a,b\in S$，有 $ab=ba$。设 S 是一个半群，且左右消去律成立，证明：S 是交换半群的充要条件是 $\forall a,b\in S,(ab)^2=a^2b^2$。

11. 证明：任意偶数阶有限群含有元素 $a\neq 1$，使 $a^2=1$。

12. 证明：群 G 不能是它的两个真子群的并。

13. 证明：$|S_n|=n!$。

14. 证明：群 G 的子集 H 成为一个子群的充要条件是 a 与 b 属于 H 时，$ab^{-1}\in H$。

15. 证明：群的任一个有限子半群必为一个子群。

16. G 是群，$a\in G$，使 $a^m=e$(单位元)的最小自然数 m 叫 a 的阶或周期，若这样的 m 不存在，称 a 的周期(阶)是无限的。证明：在有限群 G 中，周期大于 2 的元的个数一定是偶数。

17. 设 G 是一个阶为偶数的有限群，证明：G 中阶等于 2 的元的个数必是奇数。

§2.2 同构与同态

在§2.1 中列举的许多群的例子，表面上看来不同，但实质却是一样的，这种实质就是所谓的“同构”。在代数的研究中，许多抽

象的结构由于它同构于某种具体的结构,人们就会转而研究这种具体的结构;利用"同构",抽象的结构也一目了然。这是代数中常用的研究方法,这种方法在自动机、量子力学等的研究中也发挥了作用。我们先给出同构的定义。

定义 2.2.1 两个亚群$(M,p,1)$和$(M',p',1')$称为同构,如果存在双射 $\eta:M\to M'$,使得

(1) $\eta(1)=1'$;

(2) $\forall x,y\in M$,有 $\eta(xy)=\eta(x)\eta(y)$,记做 $M\cong M'$。

事实上,条件(1)可以去掉,因由 $x1=x=1x$ 可得 $\eta(x)\eta(1)=\eta(x)=\eta(1)\eta(x)$,而 η 是满射,$\eta(1)$是 M'的单位元,由单位元的惟一性,得 $\eta(1)=1'$,虽然如此,条件(1)仍放在同构的定义中,是为了今后用范畴来通观的需要。

注意,同构映射不一定是惟一的,即设 M 和 M'同构,则在这两个亚群之间可能存在多个同构映射。令 π 是所有亚群构成的类,则同构是 π 的一个等价关系。

任意一个抽象的亚群(群)同构于一个具体的变换亚群,这就是著名的 Cayley 定理。

定理 2.2.1 (Cayley 定理)

任一亚群(群)同构于一个变换亚群(变换群)。

证 仅对亚群证明,群的证明是类似的。

设$(M,p,1)$是亚群,$\forall a\in M$,令

$$a_L:M\to M$$
$$x\to ax$$

称 a_L 为左平移变换。设

$$M_L=\{a_L\mid a\in M\}$$

为所有的左平移变换的集合,则 M_L 是一个变换亚群。

事实上,$1_L:x\to 1x=x$,故 $1_L=1_M\in M_L$,又对 $\forall a_L,b_L\in$

M_L，由 M 是亚群，具有结合律，即 $a(bx)=(ab)x$，有 $(ab)_L(x)=(ab)x=a_Lb_L(x)$，故 $a_Lb_L=(ab)_L\in M_L$。

其次，令

$$\eta: M \to M_L$$
$$a \to a_L$$

显然，η 是双射，且 $\eta(1)=1_L$，$\eta(ab)=(ab)_L=a_Lb_L=\eta(a)\eta(b)$，故 η 是同构映射，即 $M\cong M_L$。

特别地，设 G 是群，若 $|G|=n$，则 $G_L\leqslant S_n$，故有下面的推论。

推论 任意 n 阶有限群同构于对称群 S_n 的一个子群。

现在转入研究同态，它是同构定义中去掉双射这一要求而得到的，尽管它出现的较晚，只是在 20 世纪四五十年代才成为研究群的重要工具，但它可应用于研究所有类型的代数结构，仍不失为一个重要的基本概念，下面我们给出它的正式定义。

定义 2.2.2 设 M 和 M' 是两个亚群，如果 η 满足：

(1) $\eta(1)=1'$；

(2) $\forall a,b\in M$，有 $\eta(ab)=\eta(a)\eta(b)$。

称 $\eta: M\to M'$ 为同态，若 M 是群，则条件(1)可以去掉。事实上，$\eta(1)=\eta(1^2)=\eta(1)^2$，两端同乘 $\eta(1)^{-1}$ 可得 $\eta(1)=1'$。

同构必为同态，但同态不一定是同构，要注意二者的区别，同态 η 不必是单射或满射。若 η 是满射，则称它为满同态；若 η 是单射，则称它为单同态；若 η 是双射，则 η 是一个同构。

判断两个同态相等，有一个常用的方法。

定理 2.2.2 设 η 和 ζ 是群 G 到群 G' 的同态，且 $G=\langle S\rangle$。如果对 $\forall s\in S$，有 $\eta(s)=\zeta(s)$，则 $\eta=\zeta$。

证 令 $G_1=\{a\in G\mid \eta(a)=\zeta(a)\}$，因 $\eta(1)=1'=\zeta(1)$，故 $1\in G_1$，且 $G_1\supset S$。又 $\forall a,b\in G$，因为

$$\eta(ab) = \eta(a)\eta(b) = \zeta(a)\zeta(b) = \zeta(ab)$$

故 $ab \in G_1$。

当 $a \in G_1$ 时,有 $\eta(a^{-1}) = (\eta(a))^{-1} = (\zeta(a))^{-1} = \zeta(a^{-1})$,故 $a^{-1} \in G_1 \Rightarrow G_1 \leqslant G$,而 $G_1 \supset S$,故 $G_1 = G$。即对 $\forall a \in G$,均有 $\eta(a) = \zeta(a)$,$\eta = \zeta$。

M 到其自身的一个同态叫 M 的自同态,M 到其自身的一个同构叫 M 的自同构,恒等映射是一个自同构。由定理 2.2.2,若 M 是亚群,则 $M_1 = \{a \in M \mid \eta(a) = a\} \leqslant M$;若 G 是群,则 $G_1 = \{a \in G \mid \eta(a) = a\} \leqslant G$。

令 $\mathrm{Aut}\, M = \{\eta \mid \eta$ 是 M 的自同构$\}$,$\forall \eta, \zeta \in \mathrm{Aut}\, M$,则对 $\forall a, b \in M$,有

$$\eta\zeta(ab) = \eta(\zeta(ab)) = \eta(\zeta(a)\zeta(b)) = \eta\zeta(a)\eta\zeta(b)$$

且

$$\eta\zeta(1) = 1, \eta^{-1}(ab) = \eta^{-1}(a)\eta^{-1}(b)$$

故 $\mathrm{Aut}\, M$ 是群,称之为 M 的自同构群。

若令 $\mathrm{End}\, M = \{\eta \mid \eta$ 是 M 的自同态$\}$,易证 $\mathrm{End}\, M$ 是亚群,称之为 M 的自同态亚群。

习题 2.2

1. 找出同构于 S_3 的 S_6 的子群。(提示:利用 S_3 的乘法表和同构映射 $a \to a_L$)
2. 设 G 是群,对 $a \in G$,定义右平移 a_R 为映射 $x \to xa$,证明:$G_R = \{a_R \mid a \in G\}$是集合 G 的一个变换群,并且 $a \to a_R^{-1}$ 是 G 到 G_R 的同构。
3. 整数加群同构于有理数加群吗?
4. 有理数加群同构于非零有理数乘群吗?

5. 在 $\mathbf{Z}$ 中，定义 $a\circ b=a+b-ab$，证明：$(\mathbf{Z},\circ,0)$是一个亚群，并且映射 $a\to 1-a$ 是乘法亚群$(\mathbf{Z},\cdot,1)$到$(\mathbf{Z},\circ,0)$的同构。
6. 证明：$f:x\to x^{-1}$是群 G 的一个自同构的充要条件是 G 是可换群。
7. 设 G 是可换群，k 是取定的正整数，命 $f:a\to a^k$，证明：f 是 G 的自同态映射，找出 $\mathrm{im}\ f$，$\ker f$。

§2.3 循环群

群的运算满足结合律，由数学归纳法可把结合律推广到任意 n 个元素相乘，即任意 n 个元素 $a_1,a_2,\cdots,a_n$ 相乘可以任意添加括号，它们都有一个惟一确定的积，记做

$$a_1a_2\cdots a_n \triangleq \prod_{i=1}^{n} a_i$$

特别地，如果所有 $a_i=a$，则把 $a_1a_2\cdots a_n$ 记为 a^n，显然下列算律成立

$$a^m a^n = a^{m+n},(a^m)^n = a^{mn}$$

若规定 $a^0=1,a^{-n}=(a^{-1})^n$，则上述算律对 $\forall\, m,n\in\mathbf{Z}$ 均成立。

群中任两个元素相乘不一定可换，但若对 $\forall\, a,b\in G$，均有 $ab=ba$，则称 G 为 Abel 群（交换群），它是以挪威数学家 Abel 的名字命名的。

设 $a\in G$，令 $C(a)=\{b\in G\mid ab=ba\}$，易证 $C(a)$是 G 的子群，称为 a 的中心化子。

设 $A\subset G$，则

$$C(A)=\bigcap_{a\in A}C(a)\leqslant G$$

$C(A)$称为 A 的中心化子。特别地，G 的中心化子 $C(G)$叫做 G 的中心，简记为 C。

在 Abel 群中，乘法的可换性由数学归纳法可推广到任意有限多个，即任意 n 个元素 $a_1,a_2,\cdots,a_n$ 相乘可以任意颠倒次序，且都有惟一结果 $a_1a_2\cdots a_n$。

特别地，在 Abel 群中，具有算律

$$(ab)^n = a^nb^n,\forall a,b\in G$$

下面，转入讨论循环群。

定义 2.3.1 由单个元素生成的群叫做循环群，记做 $G=\langle a\rangle$，其中 a 叫做生成元。

显然，$\langle a\rangle=\{a^k\mid k\in\mathbf{Z}\}$，且循环群必为 Abel 群。循环群的两个重要例子一个是整数加群 $(\mathbf{Z},+,0)=\langle 1\rangle=\langle -1\rangle$，由此可见，循环群的生成元不一定惟一；另一个是 n 次单位根群 U_n，它由 n 次单位原根 $e^{\frac{2\pi i}{n}}$ 生成，即 $U_n=\langle e^{\frac{2\pi i}{n}}\rangle$。下面证明，任何一个循环群或与 $\mathbf{Z}$ 同构，或与 U_n 同构，这就是循环群的结构定理。

定理 2.3.1 任何两个同阶循环群都是同构的。

证 设 $G=\langle a\rangle=\{a^k\mid k\in\mathbf{Z}\}$，若对 $\forall m,n\in\mathbf{Z}$，当 $m\neq n$ 时，$a^m\neq a^n$，则 G 是无限阶群。令

$$\eta:\mathbf{Z}\to G$$
$$n\to a^n$$

显然，η 是双射，且 $\eta(0)=a^0=1$，$\eta(m+n)=a^{(m+n)}=a^ma^n=\eta(m)\eta(n)$，故 η 是同构映射，即

$$\mathbf{Z}\cong G$$

若 $\exists\, m\neq n$，有 $a^m=a^n$，不妨设 $n>m$，则

$$a^{n-m}=a^na^{-m}=a^ma^{-m}=1$$

故 $\exists\, p\in\mathbf{N}$，使 $a^p=1$，设 n 是这样正整数中最小者，则必有

$$G=\{1,a,a^2,\cdots,a^{n-1}\}$$

因对 $\forall m\in\mathbf{Z}$ 均存在 q,p，使 $m=nq+p$，$0\leqslant p<n\Rightarrow a^m=a^{nq+p}=(a^n)^qa^p=a^p$，故 a^m 必为 G 中之一。又若在 $0,1,\cdots,n-1$ 中，

有 $k\neq l$，则 $a^k\neq a^l$。因若不然，取 $l>k$，得 $a^{l-k}=1$，而 $0<l-k<n$，与 n 的取法矛盾。令

$$\eta: G\to U_n$$
$$a^k\to e^{\frac{2k\pi i}{n}}$$

易证 η 是同构映射，故

$$G\cong U_n$$

运用循环群的概念可对任意群 G 的元素进行分类。$\forall a\in G$，则 $\langle a\rangle$ 是循环群，若 $|\langle a\rangle|=+\infty$，即对 $\forall m\neq 0$，有 $a^m\neq 1$，称元素 a 是无限阶的。若 $|\langle a\rangle|=r$，称元素 a 是有限阶的。这两种情况，我们均可用 $\circ(a)$ 表示 a 的阶，显然，用阶对 G 中的元素可以进行分类。

循环群是最简单的一类群，它的结构已经彻底搞清，下面继续讨论它的性质。

定理 2.3.2 循环群 $\langle a\rangle$ 的任意子群都是循环群，且若 $|\langle a\rangle|=\infty$，对 $\forall\{1\}\neq H\leqslant\langle a\rangle$，有 $|H|=\infty$。若 $|\langle a\rangle|=r<\infty$，则 $\forall H\leqslant\langle a\rangle$，$|H|\,\big|\,r$，而且对 r 的每个正因子 q 来说，有且只有一个 q 阶子群。

证 设 $H\leqslant\langle a\rangle$，若 $H=\{1\}$，显然 $H=\langle 1\rangle$，H 是循环群。现设 $H\neq\{1\}$，则 $\exists 0\neq n\in\mathbf{Z}$，使得 $a^n\in H$，而因 $a^{-n}=(a^n)^{-1}\in H$，故不妨设 $n>0$，又设 s 是使 $a^s\in H$ 的最小正整数，今断言 $H=\langle a^s\rangle$。这是因为 $\forall a^m\in H$，由 $m=qs+t$，$0\leqslant t<s$，则 $a^t=a^m(a^s)^{-q}\in H$，由 s 的最小性，必有 $t=0$，故 $a^m=(a^s)^q\in\langle a^s\rangle$，故 $H=\langle a^s\rangle$。

设 $|\langle a\rangle|=\infty$，当 $m\neq n$ 时，$a^m\neq a^n$，$m,n\in\mathbf{Z}$，因而当 $m=0,\pm1,\pm2,\cdots$ 时，a^{ms} 都互不相同，故 $|\langle a^s\rangle|=\infty$，而 s 是使 $a^s\in\langle a^s\rangle$ 的最小的正整数，对 $\forall\{1\}\neq H=\langle a^s\rangle$，$|H|=\infty$。

显然，若令

$$\mathscr{H}(\langle a\rangle) = \{H \mid H \leqslant \langle a\rangle\}$$

则

$$\varphi: N \to \mathscr{H}(\langle a\rangle)$$
$$s \to \langle a^s\rangle$$

是双射。

再证若$|\langle a\rangle| = r < \infty$,则

$$\langle a\rangle = \{1, a, a^2, \cdots, a^{r-1}\}$$

设 $H \neq \{1\}, H \leqslant \langle a\rangle$,则 $H = \langle a^s\rangle$,其中 s 是使$a^s \in H$ 的最小正整数,今断言 $s \mid r$。

事实上,若 $r = qs + t, 0 \leqslant t < r$,有 $1 = a^r = (a^s)^q a^t \Rightarrow a^t = (a^s)^{-q} \in H$,由 s 的最小性,必有 $t = 0$,故 $r = qs$,故

$$H = \{1, a^s, \cdots, a^{(q-1)s}\}$$

$|H| = q \mid r$,而当 $H = \{1\}$时,结论显然成立。

最后证明对 r 的每个正因子q,∃! q 阶子群。

令 $M = \{s \mid s$ 是r 的正因子$\}$,则

$$\eta: M \to \mathscr{H}(\langle a\rangle)$$
$$s \to \langle a^s\rangle$$

是双射。而 $r = qs$,故当 s 跑遍了 r 的所有因子时,q 也同样跑遍了r 的所有正因子,而$|\langle a^s\rangle| = q$,故对 r 的每一个正因子,∃! q 阶子群。

推论 设$|\langle a\rangle| = r < \infty$,则阶为 $q \mid r$ 的子群H 等于H_1

$$H_1 = \{b \mid b \in \langle a\rangle, b^q = 1\}$$

证 因阶为 $q \mid r$ 的子群$H = \{1, a^s, \cdots, a^{(q-1)s}\}$, $\forall\, a^{ks} \in H$,其中 $s = \dfrac{r}{q}, k = 0, 1, \cdots, q-1$,则$(a^{ks})^q = a^{kr} = 1 \Rightarrow a^{ks} \in H_1$。

又$\forall\, b \in H_1$,则 $b = a^m$,且 $b^q = 1$,故 $a^{mq} = 1 \Rightarrow mq = kr \Rightarrow m = k \cdot \dfrac{r}{q} = ks$,故 $b = (a^s)^k \in H$。

循环群必为 Abel 群，其逆是否成立呢？一般是不成立的，但若附加一定的条件，可导出有限 Abel 群是循环群的判定准则。

定理 2.3.3 设 G 是有限 Abel 群，则 G 是循环群的充要条件是对 $\forall a \in G$，$|G|$ 是满足 $a^n = 1$ 的最小正整数 n。

为证此定理，首先证明两个引理。

引理 1 设 G 是 Abel 群，$a, b \in G$，且 $\circ(a) = m$，$\circ(b) = n$，$(m, n) = 1$，则 $\langle a \rangle \cap \langle b \rangle = \{1\}$，且 $\langle a, b \rangle = \langle ab \rangle$，$\circ(ab) = mn$。

证 设 $d \in \langle a \rangle \cap \langle b \rangle \Rightarrow d = a^k = b^l \Rightarrow d^m = a^{km} = 1, d^n = b^{ln} = 1 \Rightarrow \circ(d) \mid m, \circ(d) \mid n$，又 $(m, n) = 1 \Rightarrow \circ(d) = 1 \Rightarrow d = 1$，故 $\langle a \rangle \cap \langle b \rangle = \{1\}$。

设 $r = \circ(ab)$，则 $a^r b^r = (ab)^r = 1 \Rightarrow a^r = b^{-r} \in \langle a \rangle \cap \langle b \rangle \Rightarrow a^r = 1, b^r = 1 \Rightarrow m \mid r, n \mid r \Rightarrow [m, n] \mid r$，又 $[m, n](m, n) = mn$，而 $(m, n) = 1$，故 $[m, n] = mn \Rightarrow mn \mid r = \circ(ab)$。

另一方面，$(ab)^{mn} = a^{mn} b^{mn} = 1 \Rightarrow \circ(ab) \mid mn$。

综上所述，有 $\circ(ab) = mn$。

现在考虑 $\langle a, b \rangle$，因它是 Abel 群，故

$$\langle a, b \rangle = \{a^k b^l \mid k = 1, 2, \cdots, m, l = 1, 2, \cdots, n\}$$

因此，$|\langle a, b \rangle| \leqslant mn$，但 $\langle a, b \rangle \supset \langle ab \rangle$，而 $\langle ab \rangle = mn$，故 $\langle a, b \rangle = \langle ab \rangle$。

引理 2 设 G 是有限 Abel 群，则 G 含有一个其阶可被 G 的每个元的阶整除的元素 g。

证 首先证明，若 $a, b \in G$，且 $\circ(a) = m$，$\circ(b) = n$，则 $\exists x \in G$，使 $\circ(x) = [m, n]$。

令 $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$，$n = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$，其中 $p_i (i = 1, 2, \cdots, k)$ 是不同的素数，$e_i, f_i \geqslant 0$。且若适当调动 p_i，可假定

$$e_1 \leqslant f_1, e_2 \leqslant f_2, \cdots, e_h \leqslant f_h$$

$$e_{h+1} \geqslant f_{h+1}, e_{h+2} \geqslant f_{h+2}, \cdots, e_k \geqslant f_k \quad (1 \leqslant h \leqslant k)$$

因此,若 $r=p_1^{e_1}\cdots p_k^{e_k}$,$s=p_{k+1}^{f_{k+1}}\cdots p_t^{f_t}$,则

$$[m,n]=(n/s)\cdot(m/r)=p_1^{f_1}\cdots p_k^{f_k}\cdot p_{k+1}^{e_{k+1}}\cdots p_t^{e_t}$$

且 $(n/s,m/r)=1$,$\circ(a^r)=m/r$,$\circ(b^s)=n/s$,由引理 1,令 $x=a^rb^s$,则 $\circ(x)=(m/r)\cdot(n/s)=[m,n]$。

其次,若 $c\in G$,$\circ(c)=q$,因 $[[m,n],q]=[m,n,q]$,重复上述步骤,则 $\exists\, y\in G$,使得

$$\circ(y)=[m,n,q]$$

继续上述步骤,由于 $|G|<\infty$,$\exists\, g\in G$,使得 $\circ(g)$ 是 G 的所有元素的阶的最小公倍数。

现证定理 2.3.3。

必要性　首先假定 $G=\langle g\rangle$ 是有限循环群,则 $|G|=\circ(g)$,故 $|G|$ 是使 $g^n=1$ 的最小正整数 n,对 $\forall\, g^k\in G$,也有 $(g^k)^{\circ(g)}=1$,$\circ(g)$ 也是对 G 中任意元 g^k 满足 $(g^k)^{\circ(g)}=1$ 的最小的正整数。

充分性　由引理 2,$\exists\, g\in G$,使得对 $\forall\, a\in G$,有 $a^{\circ(g)}=1\Rightarrow$ $\circ(g)$ 是使 $a^n=1$ 的最小正数 n,由条件 $\circ(g)=|G|\Rightarrow G=\langle g\rangle$。

习题 2.3

1. 设 G 是 6 阶循环群,找出 G 的一切生成元,并找出 G 的所有子群。
2. 找出 12 阶循环群的所有子群。
3. 设 $A=(a^s)$,$B=(a^t)$ 是循环群 $G=(a)$ 的两个子群,证明:$A\cap B=(a^d)$,此处 $d=[s,t]$,即为 s,t 的最小公倍数。
4. 证明:无限循环群 G 只有两个生成元。
5. 令 $G=(a)$ 是 $r(<\infty)$ 阶循环群,证明:a^m 的阶是 $[m,r]/m=r/(m,r)$。
6. 证明:r 阶循环群恰含有 $\varphi(r)$ 个元素,这里 $\varphi(r)$(Euler φ 函数)表示小于 r 而与 r 互素(即 $(r,h)=1$)的正整数 h 的个数。

7. 设 H 是 r 阶循环群 G 的 t 阶子群，$r=st$，证明：

（ⅰ）H 是 G 的元素的 s 方幂的集合；

（ⅱ）H 是能使 $h^t=1$ 的元素 h 的集合。

8. 一个群，如果它的元素都有有限阶，则把这个群叫做周期群，设 G 是有限生成的（生成元为有限个）Abel 群，又是周期群，证明：G 是有限群。

9. 证明：有理数加群 $(Q,+,0)$ 的任意有限生成子群是循环群，并用此结果证明，这样的群不同构于它和它自身的直积。

§2.4 陪集和商群

设 G 是集合 S 的一个变换群，利用 G 可在集合 S 上定义一个关系：$x\sim_G y \Leftrightarrow \exists\, \alpha\in G$，使得 $y=\alpha(x)$。

显然，这个关系是 S 中的一个等价关系（读者自行验证），称之为 G 等价关系。

由这个等价关系可决定 S 的一个分类，由 $x\in S$ 所确定的等价类 $G_x=\{y\in S \mid \exists\, \alpha\in G$，使得 $y=\alpha(x)\}$，称为 x 的 G 轨道。

特别地，若 S 只有一个轨道，则得可迁群的概念。

定义 2.4.1 设 G 是集合 S 的一个变换群，G_x 是 $x\in S$ 的一个 G 轨道，若对 $x\in S$，有 $S=G_x$，则称 G 为 S 的可迁群。

例 设 $S=\{1,2,\cdots,n\}$，S_n 是 S 的一个置换群，$\forall\, k\in S$，$S_{nk}=\{l\in S \mid \exists\, \alpha\in S_n$，使得 $l=\alpha(k)\}$，显然 $S_{nk}=S$，故 S_n 是 S 的可迁群。

利用轨道的概念，我们将给出群的子群的陪集的定义。

设 G 是一个群，$H\leqslant G$，令

$$G_L=\{g_L \mid g_L: x\rightarrow gx,\ x,g\in G\}$$

$$G_R=\{g_R \mid g_R: x\rightarrow xg,\ x,g\in G\}$$

因 $y=gx$ 与 $y=xg$ 在 G 中有解，故 $G=G_Lx=G_Rx$，因此 G_L 与 G_R 都是 G 的可迁群，令

$$H_L(G)=\{h_L \mid h_L:x\to hx, h\in H, x\in G\}$$

由 $H\leqslant G, G\cong G_L$（Cayley 定理），得

$$H_L(G)\leqslant G_L$$

故 $H_L(G)$ 也是 G 的一个变换群，由此我们得到以下陪集的定义。

定义 2.4.2 设 G 是一个群，$H\leqslant G$，并设 $x\in G$，称 x 的 $H_L(G)$ 轨道 $Hx=\{hx \mid h\in H\}$ 为 x 关于子群 H 的右陪集。

同理，可定义 x 关于子群 H 的左陪集 $xH=\{xh \mid h\in H\}$。

显然，右陪集是 G 的一个等价类，故 G 有分类

$$G=\bigcup_{x\in G}Hx$$

且映射

$$\begin{aligned}(x^{-1}y)_R: Hx &\to Hy\\ hx &\to hx(x^{-1}y)\end{aligned}$$

是双射，则任意两个右陪集 Hx 和 Hy 具有相同的基数，因 $H=H_1$ 也是一个右陪集，故

$$|Hx|=|H|, \forall x\in G$$

特别地，若 G 是有限群，则有著名的 Lagrange 定理。

定理 2.4.1 （Lagrange 定理）

有限群 G 的任一子群 H 的阶是 G 的阶的因子，且

$$|G|=|H|\cdot[G:H]$$

其中 $[G:H]$ 是 G 关于子群 H 的右陪集的个数，称为 H 在 G 中的指数。

证 设 $H\leqslant G$，则

$$G=Hx_1\cup Hx_2\cup\cdots\cup Hx_r$$

且当 $i\neq j$ 时，$Hx_i\cap Hx_j=\varnothing$，这些右陪集的个数 r 是 H 在 G 中

的指数，即$[G:H]=r$。

又因任两个右陪集的基数相同，故

$$|Hx_i|=|H| \quad (i=1,2,\cdots,r)$$

故有

$$|G|=|H|[G:H]$$

推论 设G为n阶有限群，则对$\forall x\in G$，有$x^n=1$。

证 设$\circ(x)=m$，则$x^m=1$，而$n=mr$，故

$$x^n=x^{mr}=1$$

对上述右陪集的结论完全可以转移到左陪集中。且因$\forall hx\in Hx$，$(hx)^{-1}=x^{-1}h^{-1}\in x^{-1}H$，故

$$\varphi: Hx\to x^{-1}H$$

是右陪集的集合到左陪集的集合的双射，由此得出结论：这两个集合有相同的基数，即H在G中的右陪集个数与左陪集个数相同。

利用陪集的定义，我们将给出十分重要的概念——商亚群和商群。

首先将初等数论中同余的定义推广到亚群中。

在初等数论中，设$a,b,m\in \mathbf{Z}$，称a与b关于模m同余，记做$a\equiv b(\mathrm{mod}\ m)$，是指$\exists k\in\mathbf{Z}$，使得$a-b=km$。简言之，同余关系（同余显然是一种关系）是指$a$与$b$被$m$除具有相同余数的关系；显然，它是$\mathbf{Z}$中的一个等价关系，故可将$\mathbf{Z}$进行分类。

将同余关系推广至亚群中，有如下定义。

定义 2.4.3 设M是一个亚群，M中的同余关系（仍用“$\equiv$”表示）是指可乘的等价关系，即$\forall a,a',b,b'\in M$，若$a\equiv a'$，$b\equiv b'\Rightarrow ab\equiv a'b'$。由于$\equiv$是一个等价关系，故可做商集$\overline{M}=m/\equiv=\{\bar a\mid a\in M\}$，其中$\bar a=\{b\in M\mid b\equiv a\}$，因$\equiv$是可乘的等价关系，即由

$$\bar a=\overline{a'},\bar b=\overline{b'}\Rightarrow \overline{ab}=\overline{a'b'}$$

故在$\overline{M}$中可定义一个二元运算，仍用$\cdot$表示，易证$(\overline{M},\cdot,\bar 1)$构成

一个亚群,称这个亚群为 M 关于同余"≡"的商亚群。

研究群的同余问题归结为研究已知群的一类特殊而又重要的子群,我们首先给出它的定义。

定义 2.4.4 设 G 是一个群,$N\leqslant G$,若对 $\forall g\in G$, $\forall n\in N$,均有 $g^{-1}ng\in N$,则称 N 是 G 的正规子群,记做 $N\varDelta G$。

判断群 G 的一个子群是否是正规的,有一系列判断法则,为此,先定义群 G 的两个子集 A 与 B 的积如下:

$$AB \triangleq \{ab \mid a\in A, b\in B\}$$

定理 2.4.2 若 N 是群 G 的正规子群,则下列条件等价:

(1) $\forall g\in G$, $\forall n\in N$,均有 $g^{-1}ng\in N$;

(2) $\forall g\in G$, $gN=Ng$;

(3) $\forall g\in G$,设 $g^{-1}Ng=\{g^{-1}ng \mid n\in N\}$,则 $g^{-1}Ng\subset N$;

(4) $\forall g\in G$, $g^{-1}Ng=N$。

证 先证(1)⇔(2)。

$\forall g\in G$, $\forall n\in N$, $g^{-1}ng\in N\Leftrightarrow ng\in gN\Leftrightarrow Ng\subset gN$,由 g 的任意性 $\Leftrightarrow Ng^{-1}\subset g^{-1}N\Leftrightarrow gN\subset Ng\Leftrightarrow gN=Ng$。

(1)⇔(3)是显然的。

以下证(1)⇒(4)。

$\forall g\in G$, $\forall n\in N$ 有 $g^{-1}ng\in N$,即 $g^{-1}Ng\subset N$,另一方面,$n=g(g^{-1}ng)g^{-1}$,由 g 的任意性,$n\in g^{-1}Ng$,故 $N\subset g^{-1}Ng$,得 $g^{-1}Ng=N$。

(4)⇒(1)是显然的。

群 G 的同余和 G 的正规子群之间有下述基本关系。

定理 2.4.3 设 G 是群,≡是 G 上的一个同余关系,则 $N=\bar{1}\varDelta G$。反之,设 $N\varDelta G$,并定义≡为

$$a\equiv b(\mathrm{mod}\ N)\Leftrightarrow a^{-1}b\in N$$

则≡是 G 的一个同余关系。

证 设≡是群 G 上的一个同余关系,$N=\bar{1}$,若 $\forall n_1, n_2\in N$,

则$\overline{n_1 n_2} = \overline{n_1} \cdot \overline{n_2} = \overline{1} \cdot \overline{1} = \overline{1}$,又由$\overline{n_1} \cdot \overline{n_1^{-1}} = \overline{1} = \overline{n_1^{-1}} \cdot \overline{n_1}$,得$\overline{n_1^{-1}} = \overline{n_1}^{-1} = \overline{1}^{-1} = \overline{1}$,故 $N \leqslant G$。

又$\forall g \in G, \forall n \in N, \overline{g^{-1} ng} = \overline{g^{-1}}\,\overline{ng} = \overline{g^{-1}} \cdot \overline{g} = \overline{g^{-1} g} = \overline{1}$,故 $g^{-1} ng \in N$,得 $N \triangleleft G$。

反之,设 $N \triangleleft G$,并定义$\equiv$为

$$a \equiv b (\mathrm{mod}\ N) \Leftrightarrow a^{-1} b \in N$$

这相当于 $b \in aN$,即 $b \in N_R(G)$的一个轨道,由本节开头已证,这是一个等价关系。

再证$\equiv$是可乘的。

设 $a \equiv c(\mathrm{mod}\ N), b \equiv d(\mathrm{mod}\ N)$,则

$$a^{-1} c \in N, b^{-1} d \in N$$

即$\exists n_1 \in N, a = cn_1, \exists n_2 \in N, b = dn_2$,又由 $N \triangleleft G \Rightarrow dN = Nd$,$\exists n_3 \in N$,使得 $n_1 d = dn_3$,故

$$ab = cn_1 dn_2 = cdn_3 n_2$$

从而 $ab \equiv cd(\mathrm{mod}\ N)$。

故$\equiv$是 G 中的同余关系。

将 $\overline{G} = G/\equiv(\mathrm{mod}\ N)$记为 G/N,叫 G 关于正规子群 N 的商群,G/N 中乘法定义为

$$\forall gN, hN \in G/N, gN \cdot hN = ghN$$

其中 $N = 1N$ 是G/N 的单位元,gN 的逆元是$g^{-1}N$。

每个不等于单位元的群都有两个正规子群:G 和$\{1\}$。一个群如果只有这两个正规子群,称这个群为单群。

显然,运用同余关系也可判断此群是否是单群,即一个群是单群当且仅当只有两个当然的同余:一个是相等同余,另一个是群中任两元素都等价的同余。

此外,由定义显然可得,Abel 群的任意子群都是正规子群。设 C 是G 的中心,则 C 的每个子群都是G 的正规子群。

习题 2.4

1. 证明:若 H,K 均是有限群 G 的子群,且 $H\supset K$,则 $[G:K]=[G:H][H:K]$。
2. 设 H_1 和 H_2 是 G 的子群,证明:关于 $H_1\cap H_2$ 的任一右陪集是 H_1 的一个右陪集和 H_2 的一个右陪集的交。用此结果证明庞加莱定理:设 H_1 和 H_2 在 G 中具有有限指数,则 $H_1\cap H_2$ 在 G 中的指数也是有限的。
3. 设 G 是有限生成群,H 是 G 的具有有限指数的子群,证明:H 是有限生成群。
4. 设 H 和 K 是群 G 的两个子群,证明:

   (ⅰ)映射:$x\to hxk$ 的集合是 G 的一个变换群.其中 $h\in H,k\in K$;

   (ⅱ)x 关于这个群的轨道是集合 $HxK=\{hxk\mid h\in H,k\in K\}$,叫做 x 关于 (H,K) 的双陪集;

   (ⅲ)如果 G 是有限群,则 $|HxK|=|H|[K:x^{-1}Hx\cap K]$。
5. 设 H 是群 G 中具有有限指数的子群,证明:在 G 中存在元素 $z_1,z_2,\cdots,z_r,r=[G:H]$,它既是 H 的所有右陪集的代表元,也是所有左陪集的代表元,即 G 是 Hz_i 的不相交的并,也是 z_iH 的不相交的并。(提示:对于 $g\in G$,令 $HgH=\bigcup\limits_{i=1}^{r}Hgx_i$,其中 $x_i\in H$,且当 $i\neq j$,$Hgx_i\cap Hgx_j=\varnothing$,注意,对任意 $y_i\in H$,有 $Hgx_i=Hy_igx_i$。进而证明在 H 里能够选取 x_i,y_i,使得双陪集 HgH 中的 r 个元素 y_igx_i 同时是 H 的左陪集和右陪集的代表)
6. 设 $G=\{(a,b)\mid a,b\in\mathbf{R},a\neq0\}$,其乘积规定为 $(a,b)(c,d)=(ac,ad+b)$,证明:$K=\{(1,b)\mid b\in\mathbf{R}\}$ 是 G 的正规子群,而且

$G/K \cong (\mathbf{R}^*,\cdot,1)$。($(\mathbf{R}^*,\cdot,1)$是非零实数乘法群)

7. 证明:指数为 2 的任意子群是正规的。
8. 证明:群的任意个正规子群的交是正规子群;两个正规子群 H 和 K 的积 HK 是正规子群。
9. 设 G_1 和 G_2 是单群,确定 $G_1 \times G_2$ 的正规子群。(区别 $G_1 \cong G_2$ 和 $G_1 \not\cong G_2$ 的情形)
10. 设 G_1 和 G_2 是群 G 的两个子群,α 是用 $\alpha(g_1, g_2) = g_1g_2$ 来定义的 $G_1 \times G_2$ 到 G 的映射,证明:g_1g_2 上的纤维即 $\alpha^{-1}(g_1g_2)$是数对$(g_1k, k^{-1}g_2)$的集合,其中 $k \in K = G_1 \cap G_2$,从而证明所有纤维有相同的基数,即 K 的基数。采用这个结果证明:如果 G_1 和 G_2 都是有限的,则

$$|G_1G_2| = \frac{|G_1||G_2|}{|G_1 \cap G_2|}$$

11. 设 G 是有限群,A, B 是 G 的非空子集合,证明:如果 $|A| + |B| > |G|$,则 $G = AB$。
12. 设 G 是阶为 $2k$ 的群,其中 k 为奇数,证明:G 包含着指数为 2 的子群。

§2.5 同态基本定理

本节讨论一个亚群(群)到另一个亚群(群)的同态,将导出重要的同态基本定理及由它派生的一系列同构定理。

设 M 是一个亚群,$\equiv$是 M 上的同余,$\overline{M}$ 是由$\equiv$确定的商亚群,则自然映射

$$\gamma: M \to \overline{M}$$
$$a \to \bar{a}$$

是满同态映射,这是因为 $\gamma(1) = \bar{1}, \gamma(ab) = \overline{ab} = \bar{a}\,\bar{b} = \gamma(a)$

$\gamma(b)$。今后，称 γ 为自然同态。

定理 2.5.1 （亚群和群的同态基本定理）

设 η 是亚群 M 到 M' 的一个同态映射，则 $\eta(M)$ 是 M' 的子亚群。若 M 是群，则 $\eta(M)$ 是 M' 的子群，由 η 确定的等价关系 E_η 是 M 中的同余关系，且存在惟一的同态 $\bar{\eta}:\overline{M}=M/E_\eta\to M'$，使得 $\bar{\eta}\gamma=\eta$，其中 γ 是自然同态，$\bar{\eta}$ 是单同态。

若 η 是群 M 到群 M' 的一个同态映射，则

$$\bar{1}=N=\eta^{-1}(1')\triangle M,\overline{M}=M/N$$

γ 是 M 到 M 关于正规子群 N 的商群 $\overline{M}$ 的自然同态，此时存在惟一的同态

$$\bar{\eta}:\overline{M}=M/N\to M'$$
$$aN\to\eta(a)$$

本定理的实质部分可叙述为：存在惟一的同态 $\bar{\eta}:\overline{M}=M/E_\eta\to M'$，使下图 2-1 可换。

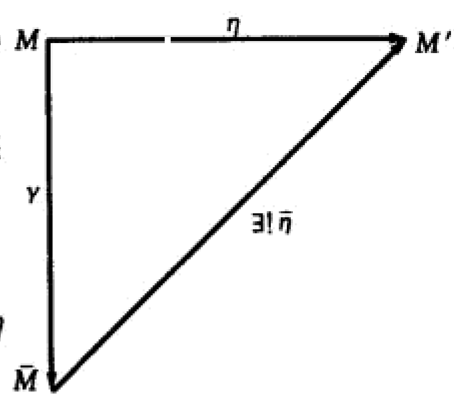


图 2-1

定理 2.5.1 的证明分成以下几个部分。

(1)令 $\eta:M\to M'$ 是一个同态映射，则

$$1'=\eta(1)\in\eta(M)$$
$$\eta(a)\eta(b)=\eta(ab)\in\eta(M)$$

故 $\eta(M)$ 是 M' 的子亚群。

当 M 是群时，有

$$(\eta(a))^{-1}=\eta(a^{-1})\in\eta(M)$$

故 $\eta(M)$ 是 M' 的子群。

(2)由 η 确定的等价关系 E_η

$$aE_\eta b\Leftrightarrow\eta(a)=\eta(b)$$

设 $a_1E_\eta a_2, b_1E_\eta b_2 \Rightarrow \eta(a_1)=\eta(a_2), \eta(b_1)=\eta(b_2) \Rightarrow$ $\eta(a_1b_1)=\eta(a_1)\eta(b_1)=\eta(a_2)\eta(b_2)=\eta(a_2b_2)\Rightarrow a_1b_1\ E_\eta\ a_2b_2$ $\Rightarrow E_\eta$ 是 M 中的同余关系。

(3)由 §1.2 得

$$\exists\,!\,\bar{\eta}: \overline{M} = M/E_\eta \to M'$$

使得 $\bar{\eta}\gamma=\eta$,下面证 $\bar{\eta}$ 是同态映射。

由 $\bar{\eta}(\bar{a})=\eta(a)\Rightarrow\bar{\eta}(\bar{a}\bar{b})=\bar{\eta}(\overline{ab})=\eta(ab)=\eta(a)\eta(b)=$ $\bar{\eta}(\bar{a})\bar{\eta}(\bar{b})$,且 $\bar{\eta}(\bar{1})=\eta(1)=1'$,由于 η 是单射,故 η 是单同态。

(4)设 M 和 M'是群,E_η 是 M 的同余关系,由定理 2.4.3 得

$$\bar{1} = N \vartriangleleft M$$

由 η 确定同余类的定义

$$\bar{1} = \{a \in M \mid \eta(a) = \eta(1) = 1'\} = \eta^{-1}(1')$$

定理的其余部分证明是显然的,定理证完。

在以上定理证明中出现的 $\bar{1}$ 是十分重要的概念,我们给出它的定义。

定义 2.5.1 设 η 是群 G 到 G'的同态映射,称

$$K = \{a \in G \mid \eta(a) = 1', 1' \text{是} G' \text{的单位元}\} = \eta^{-1}(1')$$

为同态 η 的核,记为 $\ker\,\eta$。

由群的同态基本定理可推导出 3 个同构定理。

定理 2.5.2 (第一同构定理)

设 η 是群 G 到 G'的满同态,$\ker\,\eta=K$,则

$$G/K \cong G'$$

证 首先证明 η 是单同态$\Leftrightarrow\ker\,\eta=\{1\}$。

设 $k_1,k_2\in\ker\,\eta$,则 $\eta(k_1)=1'=\eta(k_2)$,若 $\ker\,\eta\neq\{1\}$, $\exists\,k_1\neq k_2, k_1,k_2\in\ker\,\eta\Rightarrow\eta(k_1)=\eta(k_2)$,与 η 是单射矛盾。

若 $\ker\,\eta=\{1\}\Rightarrow\bar{G}=G/\ker\,\eta=G\Rightarrow$诱导同态 $\bar{\eta}$ 与 η 一致,而 $\bar{\eta}$ 是单射,故 η 是单同态。

其次，对任意同态 η，由 $\bar{\eta}\gamma=\eta$，而 γ 是满射，故 $\mathrm{im}\ \bar{\eta}=\mathrm{im}\ \eta$。因此，当 η 是满射时，$\bar{\eta}$ 也为满射，而 $\bar{\eta}$ 又是单射，故 $\bar{\eta}$ 是双射。因此，

$$G/K\cong G'$$

定理 2.5.3 （第二同构定理）

设 G 是群，$H\leqslant G$，$N\varDelta G$，则 $HN\leqslant G$，且 $HN\supset N$，$(H\cap N)\varDelta H$，有

$$H/(H\cap N)\cong HN/N$$

证 (1)$N\varDelta G\Rightarrow hN=Nh$，$h\in H$，再由 $HN=\bigcup_{h\in H}hN$，$NH=\bigcup_{h\in H}Nh\Rightarrow HN=NH$，故 $\forall\, h_1n_1, h_2n_2\in HN$，有

$$(h_1n_1)(h_2n_2)=h_1(n_1h_2)n_2=h_1h_2'n_1n_2\in HN$$

且

$$(h_1n_1)^{-1}=n_1^{-1}h_1^{-1}\in NH=HN,1\in HN$$

故

$$HN\leqslant G$$

显然 $HN\supset 1N=N$，而 $N\varDelta G$，故

$$N\varDelta HN$$

(2)令

$$\gamma: G\to G/N$$
$$g\to gN$$

取 $\gamma'=\gamma|H$，则 $\mathrm{im}\ \gamma'=\{hN\mid h\in H\}$，又 $hnN=hN(h\in H,n\in N)\Rightarrow\mathrm{im}\ \gamma'=HN/N$，$\ker\gamma'=\{h\in H\mid hN=N$，$N$ 是 HN/N 的单位元$\}$，又因 $hN=N$ 当且仅当 $h\in N$，故 $\ker\gamma'=H\cap N$，即 $(H\cap N)\varDelta H$。

(3)由第一同构定理 $H/\ker\gamma'\cong HN/N$，即

$$H/(H\cap N)\cong HN/N$$

定理 2.5.4 （第三同构定理）

设 G 是一个群，$K \triangle G$，$H \leqslant G$，且 $H \supset K$，则 $\overline{H} = H/K \leqslant \overline{G} = G/K$，且

$$f: S = \{H \mid H \leqslant G, H \supset K\} \to U = \{\overline{H} \mid \overline{H} \leqslant \overline{G}\}$$

是双射。

并且 $H \triangle G$ 的充要条件是 $\overline{H} \triangle \overline{G}$，这时有

$$G/H \cong \overline{G}/\overline{H} = G/K \big/ H/K$$

证 (1)由 G/K 的定义及 $H \leqslant G$，显然有

$$\overline{H} \leqslant \overline{G}$$

(2)令

$$f: S \to U$$
$$H \to \overline{H}$$

$\forall H_1, H_2 \in S$，若 $\overline{H}_1 = \overline{H}_2$，即 $H_1/K = H_2/K$，我们有 $\forall h_1 \in H_1 \Rightarrow h_1K \in H_1/K = H_2/K \Rightarrow \exists h_2 \in H_2$，使 $h_1K = h_2K \Rightarrow h_2^{-1}h_1 \in K \Rightarrow \exists k \in K$，使 $h_1 = h_2k$，又 $K \subset H_2 \Rightarrow h_1 \in H_2 \Rightarrow H_1 \subset H_2$。

同理 $H_2 \subset H_1 \Rightarrow H_1 = H_2$，故 f 是单射。

$\forall \overline{H} \in U$，则 $\overline{H} = \{hK \mid h \in H\}$，令

$$H = \bigcup_{h \in H} hK$$

若 $h_1, h_2 \in H \Rightarrow h_1K, h_2K \in \overline{H}$，且 $h_1h_2K = (h_1K)(h_2K) \in \overline{H} \Rightarrow h_1h_2 \in H$；同理，由 $h_1^{-1}K = (h_1K)^{-1} \in \overline{H} \Rightarrow h_1^{-1} \in H$，故 $H \leqslant G$，显然 $\overline{H} = H/K$，故 f 是满射。

(3)显然 $H \triangle G \Rightarrow \overline{H} \triangle \overline{G}$。反之，若 $\overline{H} \triangle \overline{G}$，则 $\forall h \in H, g \in G$，有 $(g^{-1}hg)K = (gK)^{-1}(hK)(gK) = h'K, h' \in H \Rightarrow g^{-1}hg \in H \Rightarrow H \triangle G$。

(4)由(3)$\overline{G}/\overline{H}$ 有意义，令

$$\bar{\gamma}: \overline{G} \to \overline{G}/\overline{H}$$
$$\bar{g} \to \bar{g}\overline{H}$$
$$\gamma: G \to \overline{G}$$

$$g \to \bar{g}$$

则

$$\bar{\gamma}\gamma : G \to \bar{G}/\bar{H}$$

$$g \to \bar{g}\bar{H}$$

$\ker(\bar{\gamma}\gamma) = \{g \mid g \in G, \bar{g} \in \bar{H}\} = \{g \in G \mid \exists h \in H \text{ 使 } gK = hK\} = H$，由第一同构定理有

$$G/H \cong \bar{G}/\bar{H} = G/K \big/ H/K$$

将第三同构定理推广，可得到以下更一般的形式。

定理 2.5.5 令 η 是群 G 到 G' 的满同态映射，设

$$\Lambda = \{H \mid H \leqslant G, H \supset \ker \eta\}, \Pi = \{H' \mid H' \leqslant G'\}$$

并设

$$\eta : \Lambda \to \Pi$$

$$H \to \eta(H)$$

则 η 是双射，且 $H \triangle G \Leftrightarrow \eta(H) \triangle G'$，并有

$$G/H \cong G'/\eta(H)$$

此定理的证明与定理 2.5.4 的证明类似，请读者自行证明。

习题 2.5

1. $a \to a^{-1}$ 是群 G 的一个自同构当且仅当 G 是 Abel 群。如果 G 是 Abel 群，则对每个 $k \in \mathbf{Z}$，$a \to a^k$ 是一个自同态。
2. 对于(ⅰ)G 是无限循环群，(ⅱ)G 是 6 阶循环群，(ⅲ)G 是任意有限循环群，确定 Aut G。
3. 设 G 是一个群，$a \in G$，定义内自同构(或共轭)，$I_a : x \to axa^{-1}$，证明：I_a 是自同构。再证明：$a \to I_a$ 是 G 到 Aut G 的同态，其核为 G 的中心 C，于是得结论：$\mathrm{I_{nn}}\, G = \{I_a \mid a \in G\}$ 是使得 $\mathrm{I_{nn}}\, G \cong G/C$ 的 Aut G 的子群。证明：$\mathrm{I_{nn}}\, G$ 是 Aut G 的正规子

群，Aut $G/I_{nn}G$ 叫做外自同构群。

4. 设 G 是群，G_L 是 G 的左平移变换 a_L 的集合，$a\in G$，证明：$G_L\text{Aut }G$ 是 G 的一个变换群，并含有 G_R，$G_L\text{Aut }G$ 称为 G 的全形，用 Hol G 表示，证明：若 G 为有限的，则 $|\text{Hol }G|=|G|\cdot|\text{Aut }G|$。

5. 设 G 是一个群，使 Aut $G=1$，证明：G 是 Abel 群且 G 的元素满足方程 $x^2=1$，并且若 G 是有限的，则 $|G|=1$ 或 2。

6. 设 α 是群 G 的仅使单位元不动的自同构（即 $\alpha(a)=a\Rightarrow a=1$），证明：$a\to\alpha(a)\cdot a^{-1}$ 是单射。由此证明：若 G 是有限的，则 G 的每一个元素都具有形式 $\alpha(a)a^{-1}$。

7. 设 G 和 α 如以上 6 题，G 是有限的，且 $\alpha^2=1$，证明：G 必是奇数阶的 Abel 群。

8. 设 $\{H_\alpha\}$ 是一簇含有正规子群 K 的子群，证明：

$$\bigcap(H_\alpha/K)=(\bigcap H_\alpha)/K$$

9. 设群 G 的子群只有有限个，f 是 G 到自身的一个满同态，证明：f 是 G 的一个自同构。

10. 设 $G=(a)$ 是 n 阶循环群，$G'=(b)$ 是 m 阶循环群，证明：当且仅当 $m\mid nk$ 时，存在 G 到 G' 的同态映射 φ，具有性质 $\varphi(a)=b^k$。设 $nk=mt$，证明：上述 φ 是单同态的充要条件是 $(n,t)=1$。

§2.6 作用于集合上的群

本节研究群在一个集合上的作用，它对于研究一些群的结构将是一个好的工具，且又是将抽象群转化成变换群的一种实现。

定义 2.6.1 群 G 叫做作用于集合 S 上，是指存在一个映射

$$T:G\times S\to S$$

$$(g,x)\to gx$$

使得对$\forall x\in S, g_1, g_2\in G$,有

(1)$1x=x$;

(2)$(g_1g_2)x=g_1(g_2x)$。

$T(g,x)$也可记做$T(g)(x)$,此时,对$\forall g\in G$,$T(g)$是S到S的映射$T(g):x\to gx$。

注意,群G在一个集合S上的作用可能有许多方式,gx仅是一个记号而已,这在实际运用中要注意,请看下面的例子。

例1 对称群S_n在集合$S=\{1,2,\cdots,n\}$上的作用由映射T给出

$$T:S_n\times S\to S$$
$$(\sigma,x)\to\sigma(x)$$

例2 G是群,$S=G$,$\forall g\in G, x\in S$,G在S上的作用由映射$T(g,x)=gx$给出,而gx被定义为g与x在G中的乘积,这个作用叫G借助于左平移在其自身上的作用,也就是曾用于Cayley定理证明时的那个作用。

例3 G到其自身的另一个作用是共轭作用

$$T(g,x)\triangleq gxg^{-1}$$

注意,相当于定义2.6.1中的gx,此处是gxg^{-1},T显然满足

$$1x1^{-1}=x$$

$$g_1g_2x(g_1g_2)^{-1}=g_1(g_2xg_2^{-1})g_1^{-1},\forall x,g_1,g_2\in G$$

例4 设G是群,$H\leqslant G$,令

$$G/H=\{xH\mid x\in G\}$$

称G/H为G关于H的左陪集空间。注意G/H不是商群,因H不一定是G的正规子群,尽管我们使用了同一个表示,在具体运用时,应看它的实质意义。令

$$T:G\times G/H\to G/H$$

$$(g, xH) \to g(xH) \triangleq gxH$$

T 满足定义 2.6.1 中的(1),(2),故定义了一个 G 到 G/H 的作用。

例 5 设群 G 作用于集合 S 上,$W \subset S$,且满足:$\forall g \in G$,$gW \subset W$,限制这个作用于 W 上,得到 G 在 W 上的作用,称这个作用为限制作用。

例 6 设群 G 作用在集合 S 上,则可诱导出 G 在 $\mathscr{P}(S)$上的作用,当 $A \neq \varnothing$ 时,定义 $gA = \{gx \mid x \in A\}$,当 $A = \varnothing$ 时,定义 $g\varnothing = \varnothing$,称这个作用为诱导作用。

关于一个群 G 的作用的等价性,有一个自然的定义。

定义 2.6.2 对于群 G 分别作用在 S 和 S'上的两个作用,若存在双射

$$\alpha: S \to S'$$
$$x \to x'$$

使得$(gx)' = gx'$,$\forall g \in G$,$\forall x \in S$,则称这两个作用是等价的。

设 G 在 S 上的作用由映射 $T(g): x \to gx$ 给出,G 在 S'上的作用由映射 $T'(g): x' \to gx'$给出,则 G 在 S 和 S'上的两个作用等价当且仅当

$$\alpha T(g) = T'(g)\alpha$$

等式 $\alpha T(g) = T'(g)\alpha$ 亦指对 $\forall g \in G$,图 2-2 是可换的。

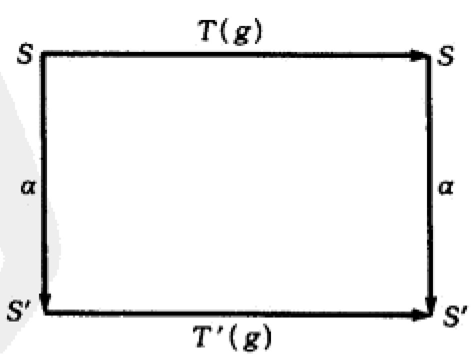


图 2-2

由于 α 是双射,两个作用等价当且仅当

$$T'(g) = \alpha T(g)\alpha^{-1}, \forall g \in G$$

例如,G 到其自身的左平移作用和右平移作用等价。

因存在双射 $\alpha: x \to x^{-1}$,使得

$$(gx)^{-1} = x^{-1}g^{-1}$$

而 $x^{-1}g^{-1}$ 恰是右平移作用中的 gx^{-1}。

设 G 作用于 S 上,对 $x,y\in S$,如果 $\exists g\in G$,有 $y=gx$,就定义一个关系 $x\sim_G y$,这个关系是一个等价关系。x 的 G 轨道是 $Gx=\{gx\mid g\in G\}$,称这些轨道的集合为 S 对 G 的商集,记做 S/G。

特别地,当 G 共轭作用于自身时,x 的 G 轨道

$$Gx=\{gxg^{-1}\mid g\in G\}$$

叫做元素 x 的共轭类。

下面讨论一类重要的作用——可迁作用。

定义 2.6.3 如果群 G 在集合 S 上的作用恰好只有一个轨道,即对某个 $x\in S$(从而也是对 $\forall x\in S$),有 $S=Gx$,称 G 是可迁地作用在 S 上。

例 7 G 到其自身的平移作用是可迁的。

例 8 G 到左陪集空间 G/H 上的作用是可迁的。

证 $\forall xH,yH\in G/H$,则 $\exists g=yx^{-1}$,使得

$$gxH=yH$$

故满足 $GxH=G/H$,这个作用是可迁的。

定义 2.6.4 设群 G 作用于集合 S 上,$\forall x\in S$,称

$$\text{stab }x\triangleq\{g\in G\mid gx=x\}$$

为 x 的稳定子。

可以证明,$\text{stab }x\leqslant G$,且在 G 到其自身的共轭作用中,$\forall x\in G$

$$\text{stab }x=\{y\in G\mid gxg^{-1}=x\}=\{g\in G\mid gx=xg\}=C(x)$$

下面的定理给出可迁作用的内在特征,它指出 G 在陪集空间 G/H 上的作用实质上是 G 仅有的可迁作用。

定理 2.6.1 设 G 可迁地作用在 S 上,对 $x\in S$,令 $H=\text{stab }x$,则 G 在 S 上的可迁作用等价于 G 在 G/H 上的作用。

证 令

$$\alpha: G \to S$$
$$g \to gx$$

由于 G 可迁地作用在 S 上，即 $Gx = \{gx \mid g \in G\} = S$，故 α 是满射，由 §1.2 得出，α 可诱导出一个由 G 的商集 $\bar{G}$ 到 S 的双射

$$\bar{\alpha}: \bar{G} \to S$$

下面证明 $\bar{G} = G/H$。

$\forall \bar{g} \in \bar{G}$，则 $\bar{g} = \{a \mid \alpha(a) = \alpha(g)\} = \{a \mid ax = gx\}$，而 $ax = gx \Leftrightarrow g^{-1}ax = x \Leftrightarrow g^{-1}a \in \text{stab } x \Leftrightarrow a \in g \text{ stab } x$。

故 $\bar{g} = g \text{ stab } x$，$\bar{G} = G/H$，即

$$\bar{\alpha}: G/H \to S$$
$$g(\text{stab } x) \to gx$$

下面证明 G 在 S 上的作用与 G 在 G/H 上的作用是等价的。

若 $g' \in G$，则由 $g'(g \text{ stab } x) = g'g(\text{ stab } x)$ 和 $g'(gx) = g'gx$ 而 $\bar{\alpha}(g'g \text{ stab } x) = g'gx$，立得

$$\bar{\alpha}(g'(g \text{ stab } x)) = g'(gx) = g'(\bar{\alpha}(g \text{ stab } x))$$

故两个作用等价。

下面转入有限群对集合 S 的作用，它将导出一个重要定理，并将成为研究有限群的得力工具。

定理 2.6.2 设 G 是可迁地作用在集合 S 上的有限群，则对 $\forall x \in S$，有 $|S| = [G:\text{stab } x]$，且 $|S| \,\big|\, |G|$，特别地，当 S 是有限集时，有 $|S| = \sum [G:\text{stab } x_i]$，其中 x_i 是 S 的元素的不同轨道的代表元，若 G 是共轭地作用于自身，有

$$|G| = \sum [G:C(x_i)]$$

其中 x_i 是 G 的共轭类的代表元。

证 (1)由定理 2.6.1

$$\bar{\alpha}: G/H \to S$$

是双射，故

$$|S| = |G/H| = [G:\text{stab } x]$$

又由 Lagrange 定理，$|G| = |G|\cdot[G:H]$，故 $|S| \mid |G|$。

(2)设 S 是有限集，S 有分类

$$S = O_1 \cup O_2 \cup \cdots \cup O_r$$

其中 O_i 是在 G 作用之下 S 的元素的不同轨道，则 G 可迁地作用于 O_i，故当 $x_i \in O_i$ 时，由(1)，$|O_i| = [G:\text{stab } x_i]$，故

$$|S| = \sum_{i=1}^{r}[G:\text{stab } x_i]$$

(3)若 G 共轭地作用于自身

$$\text{stab } x_i = C(x_i)$$

故 $|G| = \sum[G:C(x_i)]$，其中 $C(x_i)$是 x_i 的中心化子，x_i 是共轭类的代表元。

在公式 $|G| = \sum[G:C(x_i)]$中，将使 $C(x_i) = G$ 的 x_i 组成的类集中起来恰是 G 的中心 C，它们的类都含有单个元素，故 $|G| = |C| + \sum[G:C(y_i)]$，其中 y_i 跑遍了含有多于一个元素的共轭类，即$[G:C(y_i)]>1$。

称公式 $|G| = |C| + \sum[G:C(y_i)]$为有限群的类方程。

有限群的类方程是研究有限群的重要工具，请看下面的定理。

定理 2.6.3 任意阶为素数幂的有限群 G 的中心 $C \neq \{1\}$。

证 由有限群的类方程

$$|G| = |C| + \sum[G:C(y_i)]$$

设 $|G| = p^r$，p 为素数，则 $p \mid |G|$，而$[G:C(y_i)]>1$，且$[G:C(y_i)]$是 $|G|$ 的因子，并且是 p 的方幂 $\Rightarrow p \mid [G:C(y_i)] \Rightarrow p \mid |C|$，故 $C \neq \{1\}$。

可迁作用分成本原的和非本原的两种，这对今后的研究是有

用的。

设集合 S 有一个分类 $\Pi(S)$，称 $\Pi(S)$ 被 G 在 S 上的作用稳定是指 $\forall g\in G, A\in\Pi(S)\Rightarrow gA\in\Pi(S)$。显然 S 有两个平凡的分类，$\Pi_1(S)=\{S\}$，$\Pi_2(S)=\{\{x\}\mid x\in S\}$，若 $\Pi_1(S)$ 和 $\Pi_2(S)$ 是被 G 在 S 上的作用所稳定的 S 的仅有的分类，称这个作用为本原作用，而把 G 在 S 上的非平凡的和非可迁的作用称做非本原的。

习题 2.6

1. 证明：如果有限群 G 有一个指数为 n 的子群 H，则 H 包含有 G 的一个指数为 $n!$ 的因数的正规子群。（提示：考虑 G 在 G/H 上的左平移作用）
2. 设 p 是整除一个有限群的阶的最小素数，证明：G 的指数为 p 的任意子群 H 是正规子群。
3. 设 p 为素数，证明：每个阶为 p^2 的群是 Abel 群。
4. 设 H 是有限群 G 的真子群，证明：$G\neq\bigcup\limits_{g\in G}gHg^{-1}$。
5. 设 G 作用于集合 S，H 作用于集合 T，且 $S\cap T=\varnothing$，又设 $U=S\cup T$，且对 $g\in G, h\in H, s\in S, t\in T$，定义 $(g,h)s=gs$，$(g,h)t=ht$，证明：这定义了一个 $G\times H$ 在 U 上的作用。
6. 设 G 是群，H 是作用于集合 S 上的一个变换群，用 G^S 表示 S 到 G 的映射的集合，如果定义 $(f_1f_2)(s)=f_1(s)f_2(s)$，其中 $f_1, f_2\in G^S$，$s\in S$，则 G^S 是群。如果 $h\in H$，$f\in G^S$，定义 hf 为 $(hf)(s)=f(h^{-1})(s)$，证明：这是用自同构定义的 H 到 G^S 上的作用。
7. 设 G 作用于 S 上，如果对于 S^k $(\underbrace{S\times S\times\cdots\times S}_{k个})$ 中的任意两个元素 $(x_1,\cdots,x_k)$，$(y_1,\cdots,y_k)$，其中 x_i 与 y_i 不同，都存在 $g\in$

G,使得 $gx_i = y_i, 1 \leqslant i \leqslant k$,则把这个作用叫做 k 重可迁的($k = 1,2,\cdots$),证明:若 G 的作用是二重可迁的,则它必定是本原的。

8. 证明:若 G 对 S 的作用是本原的,则由 G 的正规子群导出的作用或是可迁的,或是平凡的。

§2.7 Sylow 子群

由 Lagrange 定理已经知道,有限群 G 的子群的阶是 $|G|$ 的因子,那么,其逆是否成立?即若 $k \mid |G|$,是否总存在 G 的 k 阶子群?回答是否定的。仅举一个反例,交代群 A_4 的阶为 12,但它不含 6 阶子群。但较弱的结果是成立的,即若 p 是素数,$p^k \mid |G|$,则 G 必有 p^k 阶子群,这个结果是属于 Sylow 的。关于这方面,还有几个重要的结论,我们现在来讨论这些结论。

定理 2.7.1 (Sylow 第一定理)

设 G 是有限群,p 是素数,且 $p^k \mid |G|$,$k \geqslant 0$,则 G 中存在 p^k 阶子群。

为证此定理,首先给出一个引理。

Cauchy 引理 若 G 是有限 Abel 群,p 是素数,$p \mid |G|$,则 G 中存在 p 阶元。

证 (1) 取 $a \in G, a \neq 1$,设 $|a| = r, p \mid r$,则 $\exists r'$ 使 $r = pr'$,设 $b = a^{r'} \in G$,则 $|b| = p$。

(2) 设 $|a| = r$,但 $(r,p) = 1 \Rightarrow |G/\langle a\rangle| = |G|/r$,且 $p \mid |G|/r$,由(1) $\exists b\langle a\rangle \in G/\langle a\rangle$,$|b\langle a\rangle| = p$。

设 $|b| = s$,则 $(b\langle a\rangle)^s = b^s\langle a\rangle = \langle a\rangle \Rightarrow p \mid s$,因 b 的阶可被 p 整除,再由(1),$\exists c \in G$,$|c| = p$。

现在证明 Sylow 第一定理。

对 $|G|$ 用数学归纳法。

① 当 $|G|=1$,有 $G=\{1\}$,G 的 1 阶子群是 G 本身。

② 设对任意阶小于 $|G|$ 的群,结论成立,往证群的阶为 $|G|$ 时结论仍成立。

由有限群的类方程 $|G|=|C|+\sum[G:C(y_i)]$,若 $p\nmid|C|$,而 $p\mid|G|\Rightarrow\exists j$,使得 $p\nmid[G:C(y_j)]$,又由 Lagrange 定理,$|G|=|C(y_j)|[G:C(y_j)]\Rightarrow p^k\mid|C(y_j)|$,而 $y_j\notin C$,故 $|C(y_j)|<|G|$,由归纳法假设 $C(y_j)$ 中含有 p^k 阶子群,即 G 中含有 p^k 阶子群。

若 $p\mid|C|$,由 Cauchy 引理,C 中含有 p 阶元 x,则 $|\langle x\rangle|=p$,且 $\langle x\rangle\lhd G$,$|G/\langle x\rangle|=|G|/p\Rightarrow p^{k-1}\mid|G/\langle x\rangle|$。故由归纳法假设,$G/\langle x\rangle$ 含有阶为 p^{k-1} 的子群 $H/\langle x\rangle$,此处 $H\leqslant G$,且 $H\supset\langle x\rangle$,则 $|H|=|\langle x\rangle|\cdot[H:\langle x\rangle]=p\cdot p^{k-1}=p^k$。

在 G 的所有 p^k 阶子群中,必有一个最大的,我们给出以下定义。

定义 2.7.1　设 p^m 是整除 $|G|$ 的 p 的最高次幂,则存在 G 的 p^m 阶子群 H,称 H 为 G 的 Sylow p- 子群,简记为 s. p 子群,记做 $H\overset{s.p}{\leqslant}G$。

下面专门研究 Sylow p- 子群。

令 $\Pi=\{P\mid P\overset{s.p}{\leqslant}G\}$,设 G 共轭作用在 Π 上,即对 $\forall P\in\Pi$,$g\in G$,存在映射

$$T(g):G\times\Pi\to\Pi$$

$$(g,P)\to gPg^{-1}$$

且 $\text{stab }P=\{g\mid gPg^{-1}=P\}$,称 stab P 为 P 在 G 中的正规化子,

记做 $N(P)$，显然，$N(P)\supset P$，且 $P\triangleleft N(P)$。

引理 设 $P\in\Pi$，$H\triangleleft G$，且 $|H|=p^j$，$H\subset N(P)$，则 $H\subset P$。

证 $H\triangleleft G$，而 $H\subset N(P)\Rightarrow H\triangleleft N(P)$，又 $P\triangleleft N(P)\Rightarrow HP\leqslant G$，由第二同构定理(定理 2.5.3)得 $HP/P\cong H/(H\cap P)$，即 HP/P 同构于 H 的一个商群 $\Rightarrow |HP/P|=p^k$，$k\leqslant j\Rightarrow |HP|=p^k|P|$，而 $P\overset{\text{s.p}}{\leqslant}G\Rightarrow k=0\Rightarrow HP=P\Rightarrow H\subset P$。

定理 2.7.2 (Sylow 第二定理)

G 的任意两个 Sylow p-子群是共轭的，即 $\forall P_1,P_2\in\Pi$，则 $\exists g\in G$，使得 $P_2=gP_1g^{-1}$，且对 $\forall P\in\Pi$，$|\Pi|\,\big|\,[G:P]$，$|\Pi|\equiv 1(\mathrm{mod}\ p)$。

证 设 G 共轭作用于Π下，令 Σ 是在此作用下的一个轨道，即 $\Sigma=\{gPg^{-1}\mid g\in G\}$。

若 $P\in\Pi$，将 G 在Σ上的作用限制到P上，将 Σ 分解成P轨道，这些轨道中每一个的基数是 $|P|=p^m$ 的因子，所以都是 p 的方幂。

设 $P\in\Sigma$，则$\{P\}$是惟一的基数为 1 的 P 轨道，事实上，$\forall x\in P$，若 P' 是 P 轨道，则 $xP'x^{-1}=P'\Rightarrow x\in N(P')$，故 $P\subset N(P')$，对于 P' 运用引理得 $P\subset P'$，而 $|P'|=|P|\Rightarrow P=P'$，而 Σ 可写成所有P轨道的非交并，基数为 1 的 P 轨道是惟一的，其余的 P 轨道的基数均可被 p 整除，故 $|\Sigma|\equiv 1(\mathrm{mod}\ p)$。若 $P\notin\Sigma$，则含在 Σ 中的所有P轨道的基数都能被 p 整除 $\Rightarrow p\,\big|\,|\Sigma|$，而这是不可能的，故不存在 $P\notin\Sigma$ 的情形。

因此 $\Pi=\Sigma$，说明只有一个轨道，故 G 在Π上的作用为可迁作用，而若 G 可迁地作用在Π上，则 Π 的所有稳定子共轭(习题 2.7-11)，因而 G 的任意两个 Sylow p-子群是共轭的。

由于 Π 的所有稳定子都共轭，这些共轭子群的个数为

$$|\Pi| = [G:N(P)], \forall P \in \Pi$$

而 $G \supset N(P) \supset P$，显然有

$$|\Pi| = [G:N(P)] \mid [G:P]$$

而 $\Pi = \Sigma$，故

$$|\Pi| = |\Sigma| \equiv 1 (\text{mod } p)$$

定理 2.7.3 （Sylow 第三定理）

群 G 的任意一个 p^k 阶子群必包含在一个 Sylow p-子群中。

证 将 H 在 Π 上的作用限制到 H 上，因 H 轨道的基数是 p 的方幂，且 $|\Pi| \equiv 1(\text{mod } p)$，故存在含有一个元素的轨道 $\{P\}$，$H \subset N(P)$，由引理 $H \subset P$。

习题 2.7

1. 证明：不存在阶为 148 和 56 的单群。
2. 设 p, q 为素数，证明：不存在 pq 阶单群。
3. 证明：任意 6 阶非 Abel 群同构于 S_3。
4. 决定不同构的阶为 15 的群的个数。
5. 设 u, v 是 G 的对合（G 中阶数为 2 的元），证明：若 uv 的阶为奇数，则 u, v 是共轭的；若 uv 的阶数是偶数 $2n$，则 $w = (uv)^n$ 也是对合，且 $u, v \in C(w)$。
6. 假设 G 含有偶数阶子群 H，而 H 不包含 G 的所有对合，并设对任意对合 $u \in H$，有 $C(u) \subset H$，证明：G 中任意两个对合是共轭的。

在下面 4 道题中，各符号的意义是一致的。

7. 设 $|G| = p^k m$，p 为素数，令 n 表示 G 的 p^k 阶子群的个数，设 S 是 G 的基数为 p^k 的子集的集合，G 用左平移变换作用在 S 上，若 $A \in S$，令 $H_A = \text{stab } A$，那么 H_A 也用左平移作用在 A 上，注意到在作用 H_A 之下，A 的轨道是 H_A 的一些右陪集，由

此证明：$|H_A| \mid p^k$。

8. 设 S_0 是 S 的子集，$A \in S$，使得 $|H_A| = p^k$，$\bar{S}_0$ 是 S 的子集，$B \in S$，使得 $|H_B| = p^l$，$(l < k)$，注意在 G 对 S 的作用之下，任何一个 B 的轨道的阶可被 pm 整除，从而证明

$$|S| \equiv |S_0| \pmod{pm}$$

9. 设 $A \in S_0$，$x \in A$，证明：

(ⅰ) $H_A x \subset A$，同时由 $|H_A| = p^k = |A|$，有 $H_A x = A$，因此 A 是 p^k 阶子群 H_A 的右陪集。

(ⅱ) 设 H 是任意 p^k 阶子群，Hx 是它的一个右陪集，则 $H(Hx) = Hx$。

(ⅲ) 由 $H(Hx) = Hx$ 知，$\mathrm{stab}\, Hx$ 包含 H，因此由第 7 题知 $\mathrm{stab}\, Hx = H$，则 $Hx \in S_0$。由此得出 $|S_0| = nm$。

10. 注意到 $|S|$ 只依赖于 $|G|$ 和 p^k，由第 8 题和第 9 题，$n = |S_0|/m \equiv |S|/m \pmod{p}$，因此，$n$ 的同余类 $(\bmod\ p)$ 只依赖 $|G|$ 和 p^k，而与 G 无关，考察一个 $|G|$ 阶循环群，证明：确实存在一个阶为 p^k 的子群，因而 $n \equiv 1 \pmod{p}$。

11. 证明：若群 G 可迁地作用于 $\Pi = \{P \mid \overset{s.p}{\leqslant} G\}$ 上，则 Π 的所有稳定子都是共轭的。

第 3 章　环

本章研究具有两种代数运算功能的代数结构，这两种运算不是孤立的，而是用分配律有机地结合起来。尽管本章有部分结果是前一章一些结果的平移，但由于环本身的特点，又可得到许多有别于群的别具一格的若干专门的结论。本章的后一部分将集中讨论交换整环，它的原型是整数环，因而附带地我们也得出了数论的一些结果。

§3.1　环的定义

定义 3.1.1　环是由非空集合 R 和在 R 中的两个代数运算（通常表为 $+,\cdot$）以及两个特殊元素 $0,1\in R$ 构成的，并且满足下列条件：

(1)$(R,+,0)$是 Abel 群；

(2)$(R,\cdot,1)$是亚群；

(3)分配律成立，即对 $\forall\, a,b,c\in R$，有

$$a(b+c)=ab+ac$$

$$(b+c)a=ba+ca$$

这里给出的环的定义，有些代数书中称为有单位元 1 的环。他们给出的环的定义不一定要求有单位元 1，但我们强调指出，任一无单位元的环均可嵌入一个有单位元的环中（证明放在后面的习题中），因而，关于无单位元的环的许多问题均可转入到有单位元的环中来讨论。

环显然具有 Abel 加群和乘法亚群的若干性质，我们不在此罗

列，特别指出，由于分配律的存在，它还具有一些与分配律相联系的性质。

定理 3.1.1 设 R 是环，则：

(1) $\forall a\in R$，有 $0a=a0=0$；

(2) $\forall a,b\in R$，有 $(-a)b=a(-b)=-ab$；

(3) $\forall a_i,b_j\in R$，$i=1,2,\cdots,n$，$j=1,2,\cdots,m$，有

$$\left(\sum_{i=1}^{n}a_i\right)\left(\sum_{j=1}^{m}b_j\right)=\sum_{i=1}^{n}\sum_{j=1}^{m}a_ib_j$$

(4)若 $ab=ba$，$a,b\in R$，则 $(a+b)^n=\sum_{k=1}^{n}\binom{n}{k}a^kb^{n-k}$。

证 (1) $0a=(0+0)a=0a+0a\Rightarrow 0a=0$。

(2) $ab+(-a)b=(a+(-a))b=0b=0\Rightarrow(-a)b=-(ab)$。

同理 $a(-b)=-ab$。

(3)，(4)运用归纳法容易证得。

在环的乘法亚群上附加一些条件，就得到各种类型的环。

定义 3.1.2 如果环 R 的乘法亚群是可换的，则称 R 为交换环。如果一个环 R 的非零元素集合 R^* 是 $(R,\cdot,1)$ 的子亚群，则称 R 是整环。

在交换环中，算律 $(ab)^m=a^mb^m$ 成立。

在整环 R 中，显然 $R\neq 0$，且若 $a\neq 0,b\neq 0\Rightarrow ab\neq 0$。

定义 3.1.3 环 R 中的非零元 a 叫左(右)零因子，是指存在 $b\in R$，$b\neq 0$，使得 $ab=0(ba=0)$，R 中既是左零因子又是右零因子的元素叫 R 的零因子。

显然，0 是一个当然的零因子，且若 $a\neq 0$ 是一个左零因子，而对 $b\neq 0$，有 $ab=0$，则 b 是一个非零的右零因子，故有下面的命题。

命题 3.1.1 环 $R\neq 0$ 是一个整环$\Leftrightarrow R$ 不含有非零的零因

子。

命题 3.1.1 亦可作为整环的定义,判断一个环是整环的充要条件还有如下命题。

命题 3.1.2 环 R 是整环$\Leftrightarrow R\neq 0$,且 R 中消去律成立。

环中的消去律是指

$$ab = ac, a \neq 0 \quad \Rightarrow b = c$$
$$ba = ca, a \neq 0 \quad \Rightarrow b = c$$

证 必要性 设 R 是整环,且 $ab = ac \Rightarrow a(b-c)=0$,若 $a\neq 0$必有 $b-c=0\Rightarrow b=c$,另一式同理可证。

充分性 $R\neq 0$,且消去律成立,令 $ab=0, a\neq 0$,则 $ab=a0$ 由消去律得,$b=0$,故 R 是整环。

定义 3.1.4 如果环 R 的非零元素集合 R^* 是亚群$(R,\cdot,1)$的子群,则称 R 为除环,可换的除环叫域。

显然,在除环 R 中,$1\neq 0$,且对 $\forall a\neq 0$,$\exists b\in R$,使得 $ab = ba = 1$。

环 R 的乘法亚群$(R,\cdot,1)$的可逆元的集合 U 是一个子群,称为环 R 的可逆元群,U 中的元素叫单位,以区别 U 中的单位元。

和群中一样,我们给出子环的定义。

定义 3.1.5 环的子集合 S 称为 R 的子环,如果 S 是$(R,+,0)$的一个子加群,同时 S 也是$(R,\cdot,1)$的一个子亚群。子环仍用符合 $S\leqslant R$ 表示。

显然,环 R 的子集 S 是 R 的子环$\Leftrightarrow \forall a,b\in S$,有 $a-b, ab \in S$。

环 R 的子环的交也必是子环。若 $A\subset R$,令$\langle A\rangle = \bigcap\{S \mid S\leqslant R, S\supset A\}$,则$\langle A\rangle$是 R 的一个子环,称为由 A 生成的子环。

易见,$\langle A\rangle = \{1, 0, \sum \pm a_1 a_2 \cdots a_n \mid a_i \in A, i = 1,2,\cdots, n\}$,特别地,若 $A=\{a\}$,则

$$\langle A\rangle = \{1,0,\sum_{i=1}^{m} n_i a^i \mid n_i \in \mathbf{Z}, i = 1,2,\cdots,m\}$$

环的例子很多，择其典型，列举如下。

例 1 $(\mathbf{Z},+,\cdot,0,1)$按通常定义是一个环，犹如本章开头所说，它是整环的一个原型。同样，$\mathbf{Q},\mathbf{R},\mathbf{C}$都是环。

例 2 $\mathbf{Z}[\sqrt{2}]=\{m+n\sqrt{2}\mid m,n\in\mathbf{Z}\}$是$\mathbf{R}$的一个子环。

例 3 $\mathbf{Z}[\sqrt{-1}]=\{m+n\sqrt{-1}\ m,n\in\mathbf{Z}\}$是$\mathbf{C}$的一个子环，此环称做高斯整数环。

例 4 $\Gamma=\{f\mid f$是$[0,1]$上的实值连续函数$\}$，定义

$$(f+g)x = f(x)+g(x)$$

$$(f\cdot g)x = f(x)\cdot g(x),\forall f,g\in\Gamma$$

$$0x = 0$$

$$1x = x$$

则$(\Gamma,+,\cdot,0,1)$是一个环，但不是整环。

例 5 在初等数论中的同余关系可得$\mathbf{Z}$的一个分类，对于取定的自然数m，令$\mathbf{Z}_m$为模m的剩余类构成的集合，定义

$$\bar{a}\cdot\bar{b} = \overline{ab}$$

$$\bar{a}+\bar{b} = \overline{a+b},\forall\bar{a},\bar{b}\in\mathbf{Z}_m$$

易证，这种用剩余类的代表来规定剩余类的运算，其结果与代表元的选取无关，故$(\mathbf{Z}_m,+,\cdot,\bar{0},\bar{1})$是一个环，称之为模$m$的剩余环，习惯上，记做

$$\mathbf{Z}_m = \{\bar{0},\bar{1},\bar{2},\cdots,\overline{m-1}\}$$

例 6 设R是一个环，n为正整数，定义环R上$n\times n$矩阵在如下定义运算中构成一个环，称为矩阵环，记做$M_n(R)$。即

$$M_n(R) = \{\mathbf{A} = (a_{ij})_{n\times n}\mid a_{ij}\in R\}$$

$$\mathbf{A} = (a_{ij})\in M_n(R),\mathbf{B} = (b_{ij})\in M_n(R)$$

定义

$$\mathbf{A}+\mathbf{B}=(a_{ij}+b_{ij})_{n\times n}$$

$$\mathbf{A}\cdot\mathbf{B}=\mathbf{P}=(p_{ij})_{n\times n}$$

其中

$$p_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj}$$

$M_n(R)$中的可逆元构成的群，叫线性群 $L_n(R)$。

例 7 在 $M_2(C)$中取子集 $H=\left\{\begin{pmatrix}a & b\\ -\bar{b} & \bar{a}\end{pmatrix}\middle|\ \bar{a},\bar{b}\right.$ 分别是a，b 的复共轭，即

$$\left.z=x+y\sqrt{-1}\Leftrightarrow\bar{z}=x-y\sqrt{-1}),a,b\in \mathbf{C}-\right\}$$

由共轭复数的加法和乘法定义，易证

$$H\leqslant M_2(C)$$

又 $\det\begin{pmatrix}a & b\\ -\bar{b} & \bar{a}\end{pmatrix}=a\bar{a}+b\bar{b}$，($\det \mathbf{A}$ 表示 $\mathbf{A}$ 的行列式)故

$$\det\begin{pmatrix}a & b\\ -\bar{b} & \bar{a}\end{pmatrix}=0\Leftrightarrow\begin{pmatrix}a & b\\ -\bar{b} & \bar{a}\end{pmatrix}=0_{2\times 2}$$

故 H 中每一个非零元在$M_2(C)$中都有一个逆元，即 H 是一个除环。

显然

$$\boldsymbol{i}=\begin{bmatrix}\sqrt{-1} & 0\\ 0 & -\sqrt{-1}\end{bmatrix},\boldsymbol{j}=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$$

$$\boldsymbol{k}=\begin{bmatrix}0 & \sqrt{-1}\\ \sqrt{-1} & 0\end{bmatrix},\boldsymbol{e}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

均属于 H，且可以验证

$$\boldsymbol{i}^2=\boldsymbol{j}^2=\boldsymbol{k}^2=-\boldsymbol{e}$$

$$\boldsymbol{ij}=-\boldsymbol{ji}=\boldsymbol{k},\boldsymbol{jk}=-\boldsymbol{kj}=\boldsymbol{i},\boldsymbol{ki}=-\boldsymbol{ik}=\boldsymbol{j}$$

故 H 是不可换的，我们得到一个除环但不是域的例子，称环 H 为四元数除环。

习题 3.1

1. 证明：整数对(a_1,a_2)的集合关于运算

$$(a_1,a_2)+(b_1,b_2)=(a_1+b_1)+(a_2+b_2)$$
$$(a_1,a_2)\cdot(b_1,b_2)=(a_1b_1,a_2b_2)$$

是一个有零因子的除环。

2. 证明：任何一个不仅含有一个数的有限数集关于数的加法和乘法不能构成环。

3. 设 u 是有右逆元的环的一个元素，证明下面关于 u 的 3 个条件是等价的：

(i) u 具有不只一个右逆元；

(ii) u 不是一个可逆元；

(iii) u 是一个左零因子。

4. 证明卡浦兰斯基(Kaplansky)定理：如果环的一个元素有不只一个右逆元，则它有无限个右逆元。

5. 如果环 $R\neq0$, $n>1$，证明：$M_n(R)$有不等于零的零因子；如果环 R 含有元素 a,b，使 $ab\neq0$，并设 $n>1$，证明：$M_n(R)$为非交换的。

6. 如果 $a_i(i=0,1,2,3)$都是整数，或都是奇整数的$\frac{1}{2}$，判断四元数 $a_0+a_1i+a_2j+a_3k$ 的集合J 是$M_2(\mathbf{C})$的一个子环，J 是不是一个除环。

7. 证明：(i) $\mathbf{Z}[\sqrt{2}]=\{a+\sqrt{2}b\mid a,b\in\mathbf{Z}\}$是整环。

(ii) $\mathbf{Q}[\sqrt{3}]=\{a+\sqrt{3}b\mid a,b\in\mathbf{Q}\}$是域。

8. 证明：有理数域 Q 是 $Q[i]=\{a+bi \mid a,b\in Q\}$ 的惟一真子域。

9. 证明任何有限整环是除环。

10. 设环 R 的元素 a,b 满足 $ab-1$ 是可逆元，证明：$a-b^{-1}$ 和 $(a-b^{-1})^{-1}-a^{-1}$ 也是可逆元，且有

$$((a-b^{-1})^{-1}-a^{-1})^{-1}=aba-a$$

11. 如果 G 是一个群，e 是 G 的一个元素，f 是子集 $G_1=\{x\in G \mid x\neq 1\}$ 到自身的映射，且满足：

(i) $f(yxy^{-1})=y(f(x))y^{-1}, x,y\in G$;

(ii) $f^2(x)=x$;

(iii) $f(x^{-1})=e(f(x))x^{-1}$;

(iv) $f(xy^{-1})=f((f(x)f(y^{-1}))^{-1}),\ f(y^{-1}), x,y\in G_1, x\neq y$。

证明：存在惟一的除环 D，使 $D^*=G$，且在 G 中有

$$f(x)=1-x \qquad x\in G, e=-1$$

12. 如果 R 是一个交换环，$\boldsymbol{A},\boldsymbol{B}\in M_n(R)$，且 $\boldsymbol{AB}=\boldsymbol{E}$，$\boldsymbol{E}$ 是 n 阶单位矩阵，证明：$\boldsymbol{BA}=\boldsymbol{E}$。

13. 设 R 是一个环，S 是 R 的一个子集，令

$$C(S)=\{x\in R \mid xy=yx, \forall y\in S\}$$

证明 $C(S)$ 是 R 的子环。如果 $S=R$，则称 $C=C(R)$ 为环 R 的中心。当 $S=\{e_{ij}, i,j=1,2,\cdots,n\}$ 时，求 $M_n(R)$ 中的 $C(S)$，并求出 $M_n(R)$ 的中心。

14. 如果 R 是可换环，D 是 $M_n(R)$ 中对角矩阵的集合，证明：$C(D)=D$。

15. 如果 R 是一个域，$\boldsymbol{A}\in M_n(R)$，$\boldsymbol{A}$ 是一个零因子的充要条件是 $\boldsymbol{A}$ 是不可逆的，这对任何一个交换环 R 成立吗？请解释之。

16. 在四元数除环中，设 $x=a_0+a_1i+a_2j+a_3k$，令 $N(x)=$

$\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2$，$T(x)=2\alpha_0$。证明：$x\bar{x}=N(x)$，其中 $\bar{x}=\alpha_0-\alpha_1 i-\alpha_2 j-\alpha_3 k$，并证明 x 满足二次方程 $x^2-T(x)x+N(x)=0$。

17. 设 D 是除环，C 是它的中心，S 是 D 的子除环，且 S 被每个映射 $x\to dxd^{-1}$ 所稳定，其中，$d\neq 0$，$d\in D$，证明：$S=D$ 或者 $S\subset C$。

18. 证明：任意一个无单位元的环均可嵌入一个有单位元的环 R 中。

§3.2 理想

就像正规子群在群论研究中起着主要作用一样，类似于群论中正规子群的概念，理想在环论研究中也起着重要作用。

定义 3.2.1 环 R 的一个子加群 I 叫理想，如果对 $\forall r\in R$，$a\in I\Rightarrow ar, ra\in I$。

由定义显然可得环 R 的一个非空子集 I 是理想的充要条件是：

(1) $\forall a, b\in I\Rightarrow a-b\in I$；

(2) $\forall a\in I, r\in R\Rightarrow ar, ra\in I$。

与正规子群的记法一样，I 是 R 的理想，我们仍记做 $I\vartriangleleft R$。

例 1 在整数环 $\mathbf{Z}$ 中，偶数环 $D=\{2n\mid n\in\mathbf{Z}\}\vartriangleleft\mathbf{Z}$。

例 2 取定 $n\in\mathbf{Z}$，循环子加群 $\langle n\rangle=\{kn\mid k\in\mathbf{Z}\}\vartriangleleft\mathbf{Z}$。

例 3 环 R 自身和只有零元素的集合 $\{0\}$ 是 R 的理想，这是 R 的两个当然理想，若 $I\vartriangleleft R$，且 $I\neq R$，$I\neq 0$，则称 I 为 R 的真理想。

由定义立即可得以下命题。

命题 3.2.1 令 $\{A_i\mid i\in I\}$ 是环 R 中的理想族，则 $\bigcap_{i\in I}A_i$ 也是 R 的理想。

定义 3.2.2 设 R 是一个环，$S \subset R$，定义

$$(S) = \bigcap \{I \mid I \triangle R, I \supset S\}$$

则 $(S) \triangle R$，称做由 S 生成的理想，显然它是含 S 的最小的理想。若 $S = \{a_1, a_2, \cdots, a_n\}$，称 (S) 为有限生成的理想，特别地，由一个元素生成的理想 (a) 叫主理想。

主理想 (a) 可表为

$$\left\{ \sum_{i=1}^{n} r_i a s_i \mid r_i, s_i \in R, n \in \mathbf{N}^* \right\}$$

特别地，若 R 是交换环，则

$$(a) = \{ra \mid r \in R\}$$

注意，设 I 与 J 是 R 的理想，但 $I \cup J$ 不一定是 R 的理想，但 $(I \cup J) \triangle R$。且 $(I \cup J) = I + J = \{a + b \mid a \in I, b \in J\}$，这是显然的，因 $I + J \supset (I \cup J)$，易证 $I + J \triangle R$，并被包含在含 I 与 J 的任一个理想之中。

定义 $IJ = (ab)$，其中 $a \in I, b \in J$，显然

$$IJ = \left\{ \sum_{i=1}^{m} a_i b_i \mid a_i \in I, b_i \in J, m \in \mathbf{N}^*, i = 1, 2, \cdots, m \right\}$$

命题 3.2.2 设理想序列 $I_1, I_2, \cdots$，是理想的一个升链，即 $I_1 \subset I_2 \subset \cdots$，则 $\bigcup_{j=1}^{\infty} I_j \triangle R$。

证 $\forall a, b \in \bigcup_{j=1}^{\infty} I_j$，则 $\exists j \in \mathbf{N}^*, a \in I_j$，$\exists k \in \mathbf{N}^*, b \in I_k$，取 $l = \max(j, k)$，则 $a, b \in I_l \Rightarrow a - b \in I_l$。

再者，$\forall r \in R, ra, ar \in I_j \subset \bigcup_{j=1}^{\infty} I_j$，故 $\bigcup_{j=1}^{\infty} I_j \triangle R$。

通过理想，可以给出以下判别域的一个简捷条件。

定理 3.2.1 设 R 是一个交换环，$R \neq 0$，则 R 是域的充分必要条件是 R 中的理想只能是当然理想。

证 必要性 设 $I \triangle R$，且 $I \neq 0$，若 $0 \neq a \in I \Rightarrow 1 = aa^{-1} \in I \Rightarrow$

$\forall x \in R, x = x1 \in I \Rightarrow I = R$。

充分性 设 R 中仅有的理想是 $0 = (0)$ 或 $R = (1)$，如果 $\exists 0 \neq a \in R \Rightarrow (a) \neq 0 \Rightarrow (a) = R \Rightarrow 1 \in (a) \Rightarrow \exists x \in R$，使得 $ax = 1$，而 R 是可换环 $\Rightarrow ax = xa = 1 \Rightarrow R$ 是个域。

理想在环论中起的作用与正规子群在群论中起的作用一样，因此，利用理想可以构造商环。

定义 3.2.3 设 R 是环，I 是 R 的理想，在

$$R/I = \{a + I \mid a \in R\}$$

中，定义加法和乘法

$$(a + I) + (b + I) = (a + b) + I$$

$$(a + I) \cdot (b + I) = ab + I$$

且 I 是 R/I 中的零元，$1 + I$ 是 R/I 中的单位元，则 $(R/I, +, \cdot, 0, 1)$ 是一个环，称为 R 关于理想 I 的商环。

下面转入讨论整数环 $\mathbf{Z}$ 的理想和它对应的商环 $\mathbf{Z}/I$，附带得出某些有意义的数论的结果。

将整数环 $\mathbf{Z}$ 看做加群时，它的子群是循环群

$$\langle k \rangle = \{nk \mid n \in \mathbf{Z}\} = \text{主理想}(k)$$

故 $\mathbf{Z}$ 中的每一个理想都是主理想。

显然，$(l) \supset (k) \Leftrightarrow k \in (l) \Leftrightarrow \exists m \in (l)$，使 $k = lm \Leftrightarrow l \mid k$。由此可得以下命题。

命题 3.2.3 若 $m, n \in \mathbf{Z}$，(m, n) 表示由 m 与 n 生成的理想，则 $(m, n) = (d)$，其中 d 是 m 与 n 的一个最大公约数，还有 $(m) \cap (n) = ([m, n])$，其中 $[m, n]$ 是 m 与 n 的最小公倍数。

证明是容易的，留给读者。

由于 $(k) \triangleleft \mathbf{Z}$，构造商环 $\mathbf{Z}/(k)$，由于 $(k) = (-k)$，可假定 $k \geqslant 0$，若 $k = 0$，则 $\mathbf{Z}/(k)$ 与 $\mathbf{Z}$ 等同，若 $k > 0$，则

$$\mathbf{Z}/(k) = \{\overline{0} = (k), \overline{1} = 1 + (k), \cdots, \overline{k-1} = k - 1 + (k)\} = \mathbf{Z}_k$$

定理 3.2.2 当 k 为合数时，$\mathbf{Z}/(k)$ 有非零的零因子，当 k 为

素数时，$\mathbf{Z}/(k)$是一个域。

证 设 k 为合数，则 $k=lm$，$l>1$，$m>1$，则在 $\mathbf{Z}/(k)$中，$\bar{l}\neq\bar{0}$，$\bar{m}\neq 0$，但 $\bar{l}\cdot\bar{m}=\bar{k}=\bar{0}$，故 $\mathbf{Z}/(k)$有非零的零因子。

另一方面，若 k 为素数，$\forall\,\bar{a}\in\mathbf{Z}/(k)$，$\bar{a}\neq\bar{0}$，则 $k\nmid a\Rightarrow(k,a)=1\Rightarrow\exists\,x,y\in\mathbf{Z}$，使 $ax+ky=1\Rightarrow\bar{1}=\overline{ax+ky}=\bar{a}\bar{x}+\bar{k}\,\bar{y}=\bar{a}\bar{x}$，又 $\mathbf{Z}$ 中乘法可换，故 $\mathbf{Z}/(k)$是可换环，故 $\bar{a}\bar{x}=\bar{x}\bar{a}=\bar{1}\Rightarrow(\bar{a})^{-1}=\bar{x}$，即 $\mathbf{Z}/(k)$是一个域。

显然，$k=0$ 时，$\mathbf{Z}/(k)$中的可逆元是 1 和 -1，若 $k>0$，有以下定理。

定理 3.2.3 若 $k>0$，则 $\mathbf{Z}/(k)$的可逆元群 $U(\mathbf{Z}/(k))$的元素个数为 $\varphi(k)$个，$\varphi(k)$是比 k 小且与 k 互素的正整数的个数，称之为 Euler φ 函数。

证 $\forall\,\bar{a}\in U(\mathbf{Z}/(k))$，则 $\exists\,\bar{b}\in U(\mathbf{Z}/(k))$，使 $\bar{a}\bar{b}=\bar{1}\Rightarrow ab=1+mk$，$m\in\mathbf{Z}$，此式说明 a 与 k 的任一公约数都整除 1，故 a 与 k 互素。

另一方面，若$(a,k)=1\Rightarrow\exists\,x,y\in\mathbf{Z}$，使 $ax+ky=1\Rightarrow\bar{a}\bar{x}=\bar{1}\Rightarrow\bar{a}\in U(\mathbf{Z}/(k))$。

故 $|U(\mathbf{Z}/(k))|=\varphi(k)$。

由定理 3.2.3 和 Lagrange 定理可得在数论中著名的 Euler 定理和 Fermat 定理。

定理 3.2.4 （Euler 定理）

设整数 a 与正整数 k 互素，则 $a^{\varphi(k)}\equiv 1(\mathrm{mod}\ k)$。

证 因 $U(\mathbf{Z}/(k))$是有限群，$\forall\,\bar{a}\in U(\mathbf{Z}/(k))$，得$(a,k)=1$，且 $\bar{a}^{\varphi(k)}=\bar{1}\Rightarrow a^{\varphi(k)}\equiv 1(\mathrm{mod}\ k)$。

定理 3.2.5 （Fermat 定理）

设 p 是素数，且 a 是不能被 p 整除的整数，则

$$a^{p-1}\equiv 1(\mathrm{mod}\ p)$$

证 若 p 是素数，$\varphi(p)=p-1$，故得结论。

习题 3.2

1. 如果 I,J,K 是理想,证明:$(IJ)K=I(JK)$。
2. $I(J+K)=IJ+IK$ 成立吗?
3. 如果 R 是环,I 是 R 的子加群,且 I 满足 $ba\in I(ab\in I)$,其中,$a\in R,b\in I$,则称 I 是 R 的右(左)理想。证明:环 $R\neq 0$ 是一个除环的充要条件是 0 和 R 是 R 的惟一的左(右)理想。
4. 确定由 $\{a_1,a_2,\cdots,a_n\}$ 生成的左(右)理想。
5. 如果 I 是 R 的理想,U 是 R 的可逆元群,若 $U_1=\{a\mid a\in U$,且 $a\equiv 1(\mathrm{mod}\ I)\}$,证明:$U_1$ 是 U 的正规子群。
6. 如果 I 是 R 的一个理想,证明:$M_n(I)$ 是 $M_n(R)$ 的理想,并且在 $M_n(R)$ 中每个理想都有 $M_n(I)$ 的形式,其中 I 是 R 的某个理想,并证明 $I\to M_n(I)$ 是 R 的理想集合到 $M_n(R)$ 的理想集合的双射。
7. 证明:$\mathbf{Z}/(k)$ 包含幂零元($z^n=0$)的充要条件是 k 能被一个素数的方幂整除。
8. 如果 $\mathbf{A}\in L_2(\mathbf{Z}/(p))$,证明:如果 $q=(p^2-1)(p^2-p)$,那么 $\mathbf{A}^q=1$,且对每个 $\mathbf{A}\in M_2(\mathbf{Z}/(p))$,有 $\mathbf{A}^{q+2}=\mathbf{A}^2$。
9. 令 $m=rs\in I$,验证 $(r)/(m)$ 是 $I/(m)$ 的一个理想,并证明:$I/(m)\big/(r)/(m)\cong I/(r)$。
10. 如果 A 是任一个环,则 $A^2,A^3,\cdots$ 是理想;如果 A 是 I_3 里由形如

$$\begin{pmatrix}0 & a & b\\ 0 & 0 & c\\ 0 & 0 & 0\end{pmatrix}$$

的矩阵所构成的子环,这些理想是什么?

11. 找出 E_6 的所有理想。

12. 设 p,q 是两个互异素数，$(p)\cap(q)$是 $\mathbf{Z}$ 的怎样一个理想？$(p)\cdot(q)$是怎样一个理想？

13. 在高斯整数环 $\mathbf{Z}[i]$中，$L=(2+i)$含有哪些元？商环 $\mathbf{Z}/[i]/(2+i)$含有哪些元？

14. 设 L 是环 A 的一个左理想，命

$$(L:A)=\{x\mid x\in A, xA\subseteq L\}$$

证明：$(L:A)$是 A 的理想，并且对于 A 的左理想族$\{L\alpha\mid\alpha\in\Gamma\}$来说，有

$$\bigcap_{\alpha\in\Gamma}(L\alpha:A)=(\bigcap_{\alpha\in\Gamma}L\alpha:A)$$

15. 设 R 是可换环，A 是 R 的理想，令 $N(A)=\{x\mid x\in R,\exists n\in\mathbf{Z}^+$ 使 $x^n\in A\}$，证明：$N(A)$是 R 的理想。

16. 设 R 是一个环，R 的非零左理想只有本身，证明：$R^2=0$ 或 R 是除环。

17. 设环 R 的一切非零左理想的交为 L，且 $L^2\neq 0$，证明：L 含有幂等元 e，使 $L=Re$。

18. 若环 R 的每一左理想都有左单位元，证明：R 的每一左理想都有单位元。

19. 设 R 是可换环，A 是 R 的理想，S 是 R 的子集，令$(A:S)=\{x\mid x\in R, xS\subseteq A\}$，证明：$(A:S)$是 R 的一个理想，且当理想 A,B 具有关系 $A\subseteq B$ 时，$(A:S)\subseteq(B:S)$；当集合 S,T 具有关系 $S\subseteq T$ 时，$(A:S)\subseteq(A:T)$。

20. 设环 R 的理想 A 有单位元(即存在 $e\in A$ 使 $eA=Ae=A$)，B 是 A 的理想，证明：B 也是 R 的理想。

21. 设 R 的理想 A 为幂零理想(即存在 n，$A^n=0$)，且 R/A 为幂零环，证明：R 是幂零环。

22. 设 A,B 是环 R 的幂零理想，证明：$A+B$ 是 R 的幂零理想。

23. 设 L 是环 R 的一个幂零左理想,证明:R 中存在幂零理想 A,$A \supseteq L$。

24. 设环 R 中任意两个非零理想 A,B 的积 AB 均不等于零,证明:R 的任意两个非零左理想 L,M 的积 LM 也不等于零。

25. 设环 R 中任意两个非零左理想的积均不等于零,证明:若对 R 中元素 x,有 $RxR=0$,则 $x=0$。

26. 证明:不存在整环 R,R 含有 6 个元。

27. 证明:$\mathbf{Z}/(p^n)$(p 是素数)的一切非零理想的交是一个非零理想。

§3.3 环的同态

本节中关于环的同态基本定理和环的一些同构定理与群中类似结论是平行的,我们只罗列出来,而不予证明,请读者补证。

定义 3.3.1 令 R 和 R' 是环,称映射 $\eta: R \to R'$ 是环同态,如果满足:

(1) $\forall a,b \in R, \eta(a+b)=\eta(a)+\eta(b)$;

(2) $\forall a,b \in R, \eta(ab)=\eta(a)\eta(b)$;

(3) $\eta(1)=1'$,其中 1 和 $1'$ 分别是 R 与 R' 的单位元。

和群一样,若 η 是单射,称 η 是环的单同态;若 η 是满射,称 η 是环的满同态;若 η 是双射,称 η 为环同构,且称环的单同态 $R \to R'$ 为 R 在 R' 中的嵌入,并称

$$\ker \eta = \eta^{-1}(0') = \{r \in R \mid \eta(r) = 0', 0' \text{ 是 } R' \text{ 的零元}\}$$

为同态核。

定理 3.3.1 (环同态基本定理)

设 η 是环 R 到环 R' 的一个同态,$K=\eta^{-1}(0')$ 为同态核,则 $K \vartriangleleft R$,且 $\exists !$ 同态 $\bar{\eta}: R/K \to R'$,使得 $\bar{\eta}=\eta\gamma$,其中 γ 是 R 到 R/K 的自然同态,$\bar{\eta}$ 是单同态。

定理 3.3.2 （环的第一同构定理）

设 η 是环 R 到 R' 的满同态，$\ker \eta = K$，则

$$R/K \cong R'$$

定理 3.3.3 （环的第二同构定理）

设 R 是环，$S \leqslant R$，$I \triangle R$，则 $(S+I) \leqslant R$，$I \triangle (S+I)$，$S \cap I \triangle S$，有

$$(S+I)/I \cong S/S \cap I$$

定理 3.3.4 （环的第三同构定理）

设 I 和 J 均是环 R 的理想，且 $I \subset J$，则 $J/I \triangle R/I$，且

$$R/J \cong R/I\big/J/I$$

下面的定理平行于群的第三同构定理的前半部分，叙述如下。

定理 3.3.5 设 I 是环 R 的理想，则

$$f: S = \{K \mid K \triangle R, K \supset I\} \to U = \{K/I \mid K/I \triangle R/I\}$$

是双射，从而 R/I 中每个理想具有形式 K/I，其中 $K \triangle R$，且 $K \supset I$。

下面讨论两类重要的理想——素理想和极大理想。

定义 3.3.2 设 P 是环 R 的理想，称 P 是 R 的素理想，如果对 $\forall a, b \in R$，$ab \in P \Rightarrow a \in P$ 或者 $b \in P$。

例 设 p 是素数，则 $\mathbf{Z}$ 中的主理想 (p) 是素理想，因

$$ab \in (p) \Rightarrow p \mid ab \Rightarrow p \mid a \text{ 或 } p \mid b \Rightarrow a \in (p) \text{ 或 } b \in (p)$$

刻画 P 是素理想，有下面一个充要条件。

定理 3.3.6 设 R 是可换环，理想 P 是 R 的素理想的充分必要条件是商环 R/P 是整环。

证 必要性 设 P 是 R 的素理想，则由 $(a+P)(b+P)=P \Rightarrow ab+P=P \Rightarrow ab \in P \Rightarrow a \in P$ 或 $b \in P \Rightarrow a+P=P$ 或 $b+P=P$，故 R/P 是整环。

充分性 设 R/P 是整环，由于 R/P 无零因子，从而 $ab \in P \Rightarrow ab+P=P \Rightarrow (a+P)(b+P)=P \Rightarrow a+P=P$ 或 $b+P=P \Rightarrow a \in$

P 或 $b \in P$,故 P 是 R 的素理想。

定义 3.3.3 环 R 中的理想 M 叫极大理想,是指 $M \neq R$,且对 R 中的每一个理想 N,若 $M \subset N \subset R$,则或者 $N = M$,或者 $N = R$。

简言之,M 是极大理想是指 R 无真包含 M 的 R 的真理想。

定理 3.3.7 环 R 的极大理想一定存在。

证 令 $S = \{I \mid I \triangle R, 1 \notin I\}$,因 $\{0\} \in S$,故 $S \neq \emptyset$,S 依包含关系是一个偏序集,取 S 的任一非零有序子集 $L = \{I_\alpha \mid \alpha \in \mathscr{A}, \mathscr{A}$ 为一指标集$\}$,令

$$M = \bigcup_{\alpha \in \mathscr{A}} I_\alpha$$

由命题 3.2.2 得 $M \triangle R$,且 $1 \notin M \Rightarrow M$ 是 L 的上界,由 Zorn 引理,S 有极大元 M',即 R 含有极大理想 M'。

对极大理想的刻画,也有一个定理。

定理 3.3.8 设 R 是可换环,$M \triangle R$,则 M 是 R 的极大理想的充分必要条件是 R/M 是一个域。

证 必要性 设 M 是 R 的极大理想,$\forall a + M \in R/M$,$a + M \neq M$,令 $M' = \{m + ax \mid m \in M, x \in R\}$,易证 $M' \triangle R$,且 $M' \supset M$,但 $a \in M'$ 而 $a \notin M \Rightarrow M'$ 真包含 $M \Rightarrow M' = R \Rightarrow 1 \in M' \Rightarrow \exists\, m \in M, x \in R$,使得 $m + ax = 1$,故

$$1 + M = m + ax + M = ax + M = (a + M)(x + M)$$

故 $(a + M)^{-1} = x + M$,即 R/M 是一个域。

充分性 设 R/M 是一个域,若 N 是 R 的真包含 M 的理想,则 $\exists\, a \in N, a \notin M \Rightarrow a + M \neq M \Rightarrow a + M$ 有逆元存在,即 $\exists\, x \in R$,使得

$$(a + M)(x + M) = 1 + M$$

即 $ax + M = 1 + M$,但 $a \in N, N \triangle R \Rightarrow ax \in N$,而 $M \subset N \Rightarrow ax + M \subset N \Rightarrow 1 \in N \Rightarrow N = R$,故 M 是 R 的一个极大理想。

推论 1 可换环 R 的极大理想必为素理想。

证 M 是 R 的极大理想 $\Rightarrow R/M$ 是域 $\Rightarrow R/M$ 是整环 $\Rightarrow M$ 是素理想。

推论 2 设 R 是可换环，则下列条件等价：

(1) R 是域；

(2) R 无真理想；

(3) $\{0\}$ 是 R 中的极大理想。

证 由定理 3.3.8，立得 $R\cong R/\{0\}$ 是域 $\Leftrightarrow \{0\}$ 为 R 的极大理想 $\Leftrightarrow R$ 无真理想。

在本节的最后，介绍与群和亚群的直积类似的环的直和概念，并用它来证明著名的中国剩余定理。

定义 3.3.4 设 $R_1, R_2, \cdots, R_n$ 是 n 个环，令

$$R = \prod_{i=1}^{n} R_i = \{(a_1, a_2, \cdots, a_n) \mid a_i \in R_i, i = 1, 2, \cdots, n\}$$

它的加法，乘法，0，1 的定义为

$$(a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n) = (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n)$$

$$(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n) = (a_1 b_1, a_2 b_2, \cdots, a_n b_n)$$

$$0 = (0, 0, \cdots, 0)$$

$$1 = (1, 1, \cdots, 1)$$

则 $(R, +, \cdot, 0, 1)$ 做成一个环，称之为 $R_1, R_2, \cdots, R_n$ 的直和，记做

$$R = R_1 \oplus R_2 \oplus \cdots \oplus R_n = \oplus \sum_{i=1}^{n} R_i$$

将同余关系推广至环中，即为可乘、可加的等价关系，即 $\forall a, a', b, b' \in R, a \equiv a', b \equiv b' \Rightarrow ab \equiv a'b', a + b \equiv a' + b'$。

因而，设 A 是环 R 的理想，$a, b \in R$，a 与 b 叫做模 A 同余，记做 $a \equiv b (\bmod A)$，是指 $a - b \in A$。

定理 3.3.9 （中国剩余定理）

设 $A_1, A_2, \cdots, A_n$ 是环 R 的理想，且 $A_i + A_j = R (\forall i \neq j)$，

如果 $b_1,b_2,\cdots,b_n\in R$，则 $\exists b\in R$，使得

$$b\equiv b_i(\mathrm{mod}\ A_i),i=1,2,\cdots,n$$

进而，若 c 是上面同余方程组的解 $\Leftrightarrow b\equiv c(\mathrm{mod}\ \bigcap_{i=1}^{n}A_i)$。

证 因 R 中含单位元 1，故 $R^2=R$，下面用归纳法证明。

(1)由 $A_1+A_2=R,A_1+A_3=R$，故

$$R=R^2=(A_1+A_2)(A_1+A_3)=A_1^2+A_1A_3+A_2A_1+$$
$$+A_2A_3\subset A_1+A_2A_3\subset A_1+(A_2\cap A_3)\subset R$$

故 $R=A_1+(A_2\cap A_3)$。

(2)归纳假设

$$R=A_1+\bigcap_{k=2}^{n-1}A_k$$

则

$$R=R^2=(A_1+\bigcap_{k=2}^{n-1}A_k)(A_1+A_n)\subset$$
$$A_1+\bigcap_{k=2}^{n}A_k\subset R$$

因此 $R=A_1+\bigcap_{k=2}^{n}A_k=A_1+\bigcap_{k\neq 1}A_k$。

同理 $\forall i=1,2,\cdots,n$，均有

$$R=A_i+\bigcap_{k\neq i}A_k$$

从而 $\forall i=1,2,\cdots,n,\exists a_i\in A_i,r_i\in\bigcap_{k\neq i}A_k$，使得 $b_i=a_i+r_i$，并且 $r_i\equiv b_i(\mathrm{mod}\ A_i)$。

令 $b=r_1+r_2+\cdots+r_n\in R$，则

$$b\equiv b_i(\mathrm{mod}\ A_i),i=1,2,\cdots,n$$

最后，若 $c\in R$，使得 $c\equiv b_i(\mathrm{mod}\ A_i),\forall i=1,2,\cdots,n\Leftrightarrow b\equiv c(\mathrm{mod}\ A_i)(\forall i=1,2,\cdots,n)\Leftrightarrow b-c\in A_i(\forall i=1,2,\cdots,n)\Leftrightarrow b-c\in\bigcap_{i=1}^{n}A_i$，即 $b\equiv c(\mathrm{mod}\ \bigcap_{i=1}^{n}A_i)$。

这个定理之所以命名为中国剩余定理，是因为它推广了数论中的一个结论，而我们中国的数学家早在公元前1世纪就知道这个结论了，这就是著名的“韩信点兵”问题。

推论 设 $m_1, m_2, \cdots, m_n \in \mathbf{N}^*$，且当 $i \neq j$ 时，$(m_i, m_j) = 1$，则对 $\forall b_i \in \mathbf{Z}, i = 1, 2, \cdots, n$，同余方程组 $x \equiv b_i (\mathrm{mod}\ (m_i)), i = 1, 2, \cdots, n$ 有整数解，并且解由 $(m) = (m_1 m_2 \cdots m_n)$ 惟一决定。

证 令 $A_i = (m_i)$，则 $\bigcap_{i=1}^{n} A_i = ([m_1, m_2, \cdots, m_n]) = (m)$，$\forall i \neq j, (m_i, m_j) = 1 \Rightarrow \exists k, l \in \mathbf{Z}$，使 $m_i k + m_j l = 1 \Rightarrow \forall z \in \mathbf{Z}, z = z1 = z m_i k + z m_j l \in (m_i) + (m_j) = A_i + A_j$，故 $\mathbf{Z} = A_i + A_j$。

由定理3.3.9立得结论。

习题 3.3

1. 令 η 是环 A 到它自身内的一个同态，$B = \{a \in A \mid \eta(a) = a\}$，证明：$B$ 是 A 的一个子环；如果 A 是一个除环，并且 $\eta(A) \neq 0$，则 B 是 A 的一个子除环。
2. 证明：整数集 $\mathbf{Z}$ 到它自身内仅有的同态是恒等映射和把每个元素映射到0的映射，并就有理数域证明同一结果。
3. 证明：$(2, x)$ 是素理想。
4. 证明：$(3)/(6)$ 是 $\mathbf{Z}/(6)$ 的理想，且 $\mathbf{Z}/(6) \big/ (3)/(6) \cong \mathbf{Z}/(3)$。
5. 证明：$\mathbf{Z}[i] \cong \mathbf{Z}[x]/(x^2+1)$。
6. 设环 R 的子环仅有有限个，f 是 R 到自身的满同态，证明：f 是 R 的一个自同构。
7. 找出 $\mathbf{Z}_2$ 到 $\mathbf{Z}$ 的一切同态映射。
8. φ 是环 R 到 R' 的满同态，A 是 R 的理想，则 $\varphi(A) = R'$ 当且仅当 $A + \ker \varphi = R$。
9. 设 R 是一个除环，证明：R 存在极大子域 M，即 M 是 R 的一个

子域，并且 R 的任意子域 M' 均不能真正含有 M。

10. 设 $R=\mathbf{Z}[i]$，证明：(7)是 R 的素理想。

11. 设 R 是可换环，P 是 R 的一个理想，若对于 R 的任意理想 A，B，$AB\subseteq P\Rightarrow A\subseteq P$ 或 $B\subseteq P$，证明：P 是素理想。

12. 设 R 是可换环，S 是 R 的不含零元的乘法半群，P 是 R 的与 S 的交为空集的极大理想，证明：P 是素理想。

13. 设 R 是整数环 $\mathbf{Z}$ 的同态像，证明：R 的每一子环都是理想。

14. 设 R 是一个环，R 含有子域 F，R 和 F 有共同单位元，证明：R 的任一非零同态像均含有与 F 同构的子域。

15. 设 f 是域 F 到域 F' 的同态映射，且 $f(F')\neq 0$，证明：f 是单同态。

16. 如果 I 是 R 的理想，n 是正整数，证明：$M_n(R)/M_n(I)\cong M_n(R/I)$。

17. 设 R 是一个环，若对 $\forall a\in R$，存在正整数 k，使 $ka=0$，称具有性质 $ka=0$ 的最小正整数为环 R 的特征，如果这样的数不存在，则称环的特征为无限大。如果 R 是一个具有素数特征 p 的交换环，证明：$a\rightarrow a^p$ 是 R 的一个自同态，并判断它是否是自同构映射。

18. 如果 F 是一个具有素数特征 p 的有限域，证明：$p-1 \mid |F|-1$。因此如果 $|F|$ 是偶数，那么特征为 2。

19. 如果 $R\neq 0$，且除了 R 和 0 外 R 再没有理想，则称 R 是单环。证明：一个单环的特征或者是 0 或者是素数 p。

20. 证明：一个除环的同态映射是同构映射。

21. 证明：如果 $I_1+I_2=R$，且 I_1 和 I_2 为 R 的理想，$I=I_1\cap I_2$，那么就有 $R/I\cong R/I_1\oplus R/I_2$。

22. 如果 m 和 n 是互素的整数，那么 $\varphi(mn)=\varphi(m)\varphi(n)$，$\varphi$ 是 Euler φ 函数。如果 p 是一个素数，证明：$\varphi(p^e)=p^e-p^{e-1}$，

因而如果 $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$，$p_i$ 为不同的素数，那么有

$$\varphi(n)=\prod_{i=1}^{r}(p^{e_i}-p^{e_i-1})=n\prod_{i=1}^{r}(1-\frac{1}{p_i})$$

23. 设 $P_1\supseteq P_2\supseteq P_3\supseteq\cdots$ 是可换环 R 中素理想的降链，证明：$P=\bigcap_{i=1}^{\infty}P_i$ 是 R 的素理想。

§3.4 分式域

我们知道，任一除环必为整环，而整环的子环必为整环，故一个除环的任一子环是整环。其逆是否成立这个问题直到 A. Malcev 举出反例之前一直没有解决。A. Malcev 的反例说明，任一整环不一定可嵌入一个除环中，但将整环的条件加以限制就可得到任一交换整环都可嵌入一个域中这一重要的结论。我们来讨论它。

首先注意，整环的一个重要原型是整数环 Z，用它去构造有理数域 Q 的方法会给我们以很大的启示。

在 $\mathbf{Z}\times\mathbf{Z}^*$ 上定义关系

$$(a,b)\sim(c,d)\Leftrightarrow ad=bc$$

易证这是等价关系，令

$$a/b=\{(c,d)\mid(c,d)\sim(a,b)\}$$

$$\mathbf{Q}=\{a/b\mid a\in\mathbf{Z},b\in\mathbf{Z}^*\}$$

并按通常的分数的加法和乘法定义 Q 中的加法和乘法，可证(Q，+，·，0，1)是一个域。令

$$\varphi:\mathbf{Z}\to\mathbf{Q}$$

$$a\to a/1$$

则 φ 是单同态，故 Z 可嵌入有理数域 Q 中。

将 Z 嵌入 Q 中的方法可以推广到任意交换整环 D。

定理 3.4.1 任一交换整环 D 均可嵌入一个域中。

在 $D\times D^*$ 中引入关系

$$(a,b)\sim(c,d)\Leftrightarrow ad=bc$$

易证这是一个等价关系，令

$$a/b=\{(c,d)\mid(c,d)\sim(a,b)\}$$

为 (a,b) 所在的等价类，称其为分式，令

$$F=\{a/b\mid a\in D,b\in D^*\}$$

定义

$$a/b+c/d=(ad+bc)/bd$$

$$(a/b)\cdot(c/d)=(ac)/(bd)$$

可证这样定义的运算与代表元的选取无关，仅以加法为例证明，乘法同理可证。

设 $a/b=a'/b',c/d=c'/d'\Rightarrow ab'=ba',cd'=dc'\Rightarrow ab'dd'=ba'dd',cd'bb'=dc'bb'\Rightarrow ab'dd'+cd'bb'=ba'dd'+dc'bb'\Rightarrow(ad+bc)/bd=(a'd'+b'c')/b'd'$。

再定义 $0=0/1,1=1/1$，则

$$(F,+,\cdot,0,1)$$

是一个交换环。

$\forall 0\neq a/b\in F\Rightarrow a\neq 0$，即 b/a 是分式 $\Rightarrow(a/b)\cdot(b/a)=(ab)/(ab)=1/1=1\Rightarrow(a/b)^{-1}=b/a\Rightarrow F$ 是一个域。

令

$$\eta: D\to F$$
$$a\to a/1$$

则 $\eta(0)=0,\eta(1)=1$，且

$$\eta(a+b)=(a+b)/1=a/1+b/1=\eta(a)+\eta(b)$$

$$\eta(ab)=ab/1=(a/1)\cdot(b/1)=\eta(a)\cdot\eta(b)$$

故 η 是同态，且若 $a/1=0/1\Rightarrow a1=10=0\Rightarrow a=0\Rightarrow\ker\eta=\{0\}\Rightarrow\eta$ 是单同态。

D 可嵌入域 F 中，即认为 D 与 F 中的一子环等同，故 $\forall a/b \in F$，有 $a/b=(a/1)(1/b)=(a/1)(b/1)^{-1}$ 等同于 ab^{-1}。而由 D 生成的子域恰为 $\{ab^{-1} \mid a\in D, b\in D^*\}$，故称 F 为 D 的分式域。

分式域的基本性质由下面的定理给出。

定理 3.4.2 设 D 是一个交换整环，F 是它的分式域，则 D 到一个域 F' 的任一单同态 η_D 可惟一地扩张为 F 到 F' 的单同态 η_F。

证 (1)存在性

设

$$\eta_D: D \to F'$$
$$a \to a'$$

扩张为

$$\eta_F: F \to F'$$
$$ab^{-1} \to a'(b')^{-1}$$

下面证明 η_F 确为单同态。

首先，设 $ab^{-1}=cd^{-1} \Rightarrow ad=bc \Rightarrow a'd'=b'c'$（因 η_D 是同态）$\Rightarrow a'(b')^{-1}=c'(d')^{-1}$，故 η_F 确是映射。

其次，$\forall a,c\in D, b,d\in D^*$，有

$$\eta_F(ab^{-1}+cd^{-1}) =$$
$$\eta_F[(ad+bc)(bd)^{-1}] =$$
$$(ad+bc)'((bd)')^{-1} =$$
$$(a'd'+b'c')\cdot(d')^{-1}(b')^{-1} =$$
$$a'(b')^{-1}+c'(d')^{-1} =$$
$$\eta_F(ab^{-1})+\eta_F(cd^{-1})$$

同理，$\eta_F[(ab^{-1})(cd^{-1})]=\eta_F(ab^{-1})\cdot\eta_F(cd^{-1})$。

又 F 与 D 有相同的单位元，$\eta_F(1)=\eta_D(1)=1'$，故 η_F 是同态，而域的任一同态必为单同态，得 η_F 是单同态。

(2)惟一性

若 $b\in D^{*}$，$\eta_F: b^{-1}\to(b')^{-1}$，而 F 中每个元均可写做 ab^{-1}，η_F 就被 $ab^{-1}\to a'(b')^{-1}$ 完全确定。

(3) η_F 确为 η_D 的扩张

$\forall a\in D, \eta_F(a)=\eta_F(a\cdot 1^{-1})=a'(1')^{-1}=a'\Rightarrow \eta_F|_D=\eta_D$，即 η_F 是 η_D 的扩张。

习题 3.4

1. 设 A 是一个环，令 $\bar{A}=\mathbf{Z}\times A$，对 $\bar{A}$ 规定加法与乘法
$$(m,a)+(n,b)=(m+n,a+b)$$
$$(m,a)\cdot(n,b)=(mn,na+mb+ab)$$
证明：$\bar{A}$ 是环，且 $\bar{A}$ 含有子环与 A 同构。
2. 设 A 是域，证明：A 的分式域就是 A 自身。
3. 如果 D 是一个整环，F_1 和 F_2 是域，且 D 是 F_1 和 F_2 的子环，同时 F_1 和 F_2 都由 D 生成，证明：在 F_1 到 F_2 中有惟一的同构映射使其在 D 上为恒等映射。
4. 证明：任何一个满足消去律($ab=ac\Rightarrow b=c$)的交换亚群能被嵌入到一个 Abel 群中。
5. 设 D 是一个整环(不一定可交换)，对 D 中的任何两个非零元 a,b，都有 $m=ab_1=ba_1\neq0$，考虑 $D\times D^{*}$，D^{*} 是 D 的非零元素的集合，如果 $b_1\neq0, a_1\neq0$ 使得 $ba_1=ab_1, ad_1=cb_1$，那么 $(a,b)\sim(c,d)$。证明：这与 b_1,d_1 的选择无关，$\sim$ 是 $D\times D^{*}$ 的等价关系。设 F 是等价类 a/b 的集合，证明：F 在 $a/b+c/d=(ad_1+cb_1)/m\,(m=bd_1=db_1\neq0)$，$0=0/1$，$1=1/1$，$(a/b)\cdot(c/d)=(ac_1)/(db_1)\,(b_1\neq0, cb_1=bc_1)$ 下是一个除环。证明：$a\to a/1$ 是 D 到 F 的单同态映射，F 是具有形如 $(a/1)(b/1)^{-1}$

的元素的集合，其中 $a,b\in D,b\neq 0$。

§3.5 析因环

本节要把整数环 $\mathbf{Z}$ 中的可除性、最大公因子和素数等概念推广到任意交换环上，并研究一类具有惟一因子分解的整环，我们称之为析因环。

本节的环 R 若不特殊声明，均指交换环。

定义 3.5.1 对环 R 中的非零元 a，如果 $\exists x\in R$，使得 $ax=b,b\in R$，就叫 a 整除 b，并记做 $a|b$。

若 $a|b$ 且 $b|a$，称 a 与 b 相伴，记做 $a\sim b$。显然，相伴关系是 R 中的等价关系。

关于整除性的一些命题可用主理想来叙述。

定理 3.5.1 设 $a,b,u\in R$。

(1) $a|b\Leftrightarrow(b)\subset(a)$;

(2) $a\sim b\Leftrightarrow(a)=(b)$;

(3) u 是单位 $\Leftrightarrow\forall r\in R,u|r$;

(4) u 是单位 $\Leftrightarrow(u)=R$。

证 (1) $a|b\Leftrightarrow\exists x\in R$，使 $ax=b\Leftrightarrow b\in(a)\Leftrightarrow(b)\subset(a)$。

(2) $a\sim b\Leftrightarrow a|b$ 且 $b|a\Leftrightarrow(a)\subset(b)$ 且 $(b)\subset(a)\Leftrightarrow(a)=(b)$。

(3) u 是单位 $\Leftrightarrow\exists v\in R$，使 $uv=1\Leftrightarrow\forall r\in R,r=r\cdot 1=r\cdot uv\Leftrightarrow u|r$。

(4) u 是单位 $\Leftrightarrow(u)=(1)=R$。

定义 3.5.2 环 R 中的元素 c 叫不可约元素，如果：

(1) c 是非零元且不是单位；

(2) $c=ab\Rightarrow a$ 是单位或 b 是单位。

R 中的元素 p 叫素元，如果：

(1) $p\neq 0$，p 不是单位；

(2)$p\mid ab \Rightarrow p\mid a$ 或 $p\mid b$。

由定义 3.5.2 立得，c 是不可约元$\Leftrightarrow c$ 不是单位，且 c 无真因子。p 是素元$\Leftrightarrow p\nmid a$ 和 $p\nmid b \Rightarrow p\nmid ab$。

定义 3.5.3 一个整环，若每个理想都是主理想，称这个整环为主理想整环。

定理 3.5.2 设 p 和 c 是 R 中的非零元。

(1)p 为素元$\Leftrightarrow(p)$是非零素理想；

(2)R 的每个素元必为不可约元，其逆不成立，但若 R 是主理想整环，则其逆成立。

证 (1)由素元和素理想的定义立得。

(2)若 p 是素元，则 p 不是单位，$p\neq 0$，若 $p=ab$，则 $p\mid ab\Rightarrow p\mid a$ 或 $p\mid b$。若 $p\mid a$，$\exists x\in R$，使 $px=a$，而 $p=ab\Rightarrow p=ab=pxb\Rightarrow xb=1\Rightarrow b$ 是单位。同理，若 $p\mid b$，则 a 是单位，故 p 是不可约元。

其逆一般不成立。例如，在 $\mathbf{Z}[\sqrt{-5}]$中，3 是一个不可约元，但 3 不是素元，但若 R 是主理想整环，其逆一定成立，证明如下。

若 p 是不可约元，则 p 不是单位，故(p)是 R 的真理想。任取 R 的一个理想，它必为主理想，设为(d)，若$(p)\subset(d)\Rightarrow d\mid p\Rightarrow \exists x\in R$，使 $p=dx$，由 p 是不可约元，若 d 是单位，则$(d)=R$；若 x 是单位，则 $p\sim d$，即$(p)=(d)$。故(p)是 R 的极大理想，必为素理想，故 p 是素元。

我们知道，在整数环中，每一个不等于 ±1 的整数，都能分解成素数的乘积，且除了因子次序和 ±1 的因子差别外这个分解是惟一的，但这个结论不能推广到一般的整环中，例如，在 $\mathbf{Z}[\sqrt{-5}]$中，$9=3\cdot3=(2+\sqrt{-5})(2-\sqrt{-5})$。易证 $\mathbf{Z}[\sqrt{-5}]\subset\mathbf{C}$，除环的子环必为整环，故 $\mathbf{Z}[\sqrt{-5}]$是整环，且可以证明 $3,2+\sqrt{-5},2-[\sqrt{-5}]$均是 $\mathbf{Z}[\sqrt{-5}]$的不可约元，故在 $\mathbf{Z}[\sqrt{-5}]$中，分解不是

惟一的，为此，我们给出以下定义。

定义 3.5.4 整环 D 叫析因环，如果 D 中每一非单位的元素均可惟一地分解成不可约元素的乘积。

这里的惟一性是指，若

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

则 $n = m$，且适当调动次序，有 $p_i \sim q_i, i = 1, 2, \cdots, n$。

下面我们指出两类特殊的整环——主理想整环和欧氏环，它们均是析因环。

定理 3.5.3 任一主理想整环是析因环。

先证一个引理。

引理 在主理想环 R 中不含无限的主理想真升链，即设 $(a_1) \subset (a_2) \subset \cdots$ 是 R 中的升链，则 $\exists n \in \mathbf{N}^*$，使得当 $j \geqslant n$ 时，$(a_j) = (a_n)$。

证 令 $A = \bigcup_{i=1}^{\infty} (a_i)$，则 $A \triangle R$，而 R 是主理想，故 $A = (a)$，由 $a \in A = \bigcup_{i=1}^{\infty} (a_i) \Rightarrow \exists n \in \mathbf{N}^*$，使得 $a \in (a_n) \Rightarrow (a) \subset (a_n)$，故当 $j \geqslant n$ 时，$(a) \subset (a_n) \subset (a_j) \subset A = (a)$。因此

$$(a_j) = (a_n)$$

这个条件等价于因子链条件：主理想环 R 不含元素 $a_1, a_2, \cdots$ 的无限序列，使得每个 a_{i+1} 是 a_i 的真因子。

也等价于，如果 R 中不含无限的真因子序列，即设在 a_1，$a_2, \cdots$ 中，若 $a_{i+1} \mid a_i$，则 $\exists n \in \mathbf{N}^*$，使得 $a_n \sim a_{n+1} \sim a_{n+2} \sim \cdots$。

现证定理 3.5.3。

设 R 是主理想整环，令 $S = \{r \in R \mid r$ 不是单位，且 r 不能写成有限个不可约元的乘积$\}$，若 $S \neq \varnothing$，$\exists a \in S$，a 不是单位，则 (a) 是 R 的真理想。又 R 的极大理想必存在，设为 (c)，则 c 不是单位，若 $c = ab \Rightarrow (c) \subset (a) \Rightarrow (c) = (a)$ 或 $(a) = R$。若 $(a) = R$，

则 a 是单位，若 $(c)=(a)\Rightarrow c=ab=cyb\Rightarrow 1=yb\Rightarrow b$ 是单位，故 c 是不可约元。

又 $(a)\subset(c)\Rightarrow c\mid a\Rightarrow\forall a\in S$，由选择公理，均可选取 a 的一个不可约因子 c_a，由 c_a 惟一决定一个非零元 $x_a\in R$，使得 $c_a x_a=a$。

现证 $x_a\in S$。

若 x_a 是单位 $\Rightarrow a=c_a x_a$ 是不可约元；若 x_a 不是单位，且 $x_a\notin S\Rightarrow x_a$ 可分解成有限个不可约元的乘积 $\Rightarrow a$ 也可分解成有限个不可约元的乘积，与 $a\in S$ 矛盾，故 $x_a\in S$。

又因为 $x_a\mid a\Rightarrow(a)\subset(x_a)$，若 $(a)=(x_a)\Rightarrow\exists y\in R, x_a=ay\Rightarrow a=x_a c_a=ayc_a\Rightarrow yc_a=1\Rightarrow c_a$ 是单位，与 c_a 不可约矛盾，故

$$(a)\subsetneqq(x_a)$$

上述事实表明，$\exists f:S\to S, f(a)=x_a$，由递归定理，取 $f=f_n, \forall n\in N, \exists\varphi:N\to S$，使得

$$\varphi(0)=a, \varphi(n+1)=f(\varphi(n))=x_{\varphi(n)}\quad(n\geqslant 0)$$

记 $\varphi(n)=a_n$，得 S 中元素序列 $a, a_1, a_2, \cdots$，使得

$$a_1=x_a;\quad a_2=x_{a_1},\cdots;\quad a_{n+1}=x_{a_n},\cdots$$

故存在理想的真升链

$$(a)\subsetneqq(a_1)\subsetneqq(a_2)\subsetneqq\cdots$$

与引理矛盾。故 $S=\varnothing$，即 R 中每个非单位元均可分解成有限个不可约元的乘积。

最后证明惟一性。

若 a 有两种分解，即 $a=p_1p_2\cdots p_m=q_1q_2\cdots q_n$，$p_1$ 是不可约元，由定理 2.5.3，p_1 必为素元 $\Rightarrow\exists i, 1\leqslant i\leqslant n, p_1\mid q_i$，适当调动 $q_1, q_2, \cdots, q_n$ 次序，不妨设 $p_1\mid q_1$，因 q_1 也为不可约元，故 $p_1\sim q_1\Rightarrow p_1=\epsilon_1 q_1$，$\epsilon_1$ 是单位，代入上式消去 q_1，得 $p_2\cdots p_m=(\epsilon_1 q_2)$

$\cdots q_n$，再由归纳法立得 $m=n$，并适当调整顺序，有 $p_i \sim q_i$，$i=1,2,\cdots,n$。

定义 3.5.5 设 D 是整环，称 D 为欧氏环，如果存在映射 $\delta: D^* \to N$，适合条件：如果取定 $b \in D^*$，则对 $\forall a \in D$，均存在 $q, r \in D$，使得 $a = qb + r$，其中 $r=0$ 或 $\delta(r) < \delta(b)$。

例 1 整数环 $\mathbf{Z}$ 对 $\delta(x)=|x|$ 是欧氏环。

例 2 域 F 对 $\delta(x)=1(\forall x \in F^*)$ 是欧氏环。

例 3 令 $\mathbf{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbf{Z}\}$，它是高斯整数环，令 $\delta(a + b\sqrt{-1}) = a^2 + b^2$，则高斯整数环是欧氏环，证明如下。

首先 δ 是 $(\mathbf{Z}[\sqrt{-1}])^*$ 到 $\mathbf{N}$ 的一个映射，若令

$$\alpha = a + b\sqrt{-1}, \beta = c + d\sqrt{-1}$$

有 $\delta(\alpha\beta) = \delta(\alpha)\delta(\beta)$。

若 $\beta \neq 0$，则 $\alpha\beta^{-1} = u + v\sqrt{-1}$，其中 $u, v \in \mathbf{Q}$，取 u', v' 分别是与 u, v 最接近的整数，有

$$|u - u'| \leqslant \frac{1}{2}, |v - v'| \leqslant \frac{1}{2}$$

取 $\varepsilon = u - u'$，$\eta = v - v'$，则 $|\varepsilon| \leqslant \frac{1}{2}$，$|\eta| \leqslant \frac{1}{2}$，故

$$\alpha = \beta[(u' + \varepsilon) + (v' + \eta)i] \triangleq \beta q + r$$

其中 $q = u' + v'i \in \mathbf{Z}[i]$，$r = \beta(\varepsilon + \eta i)$，而 $r = \alpha - \beta q$，故 $r \in \mathbf{Z}[i]$，且

$$\delta(r) = \delta(\beta)\delta(\varepsilon + \eta i) = \delta(\beta)(\varepsilon^2 + \eta^2) \leqslant \frac{1}{2}\delta(\beta) < \delta(\beta)$$

故 $\mathbf{Z}[\sqrt{-1}]$ 是欧氏环。

定理 3.5.4 欧氏环是主理想整环，从而是析因环。

证 设 D 是欧氏环，$I \triangleleft D$，若 $I=0$，则 $I=\{0\}$，若 $I \neq \{0\}$，

令 $A=\{\delta(x)\mid x\in I,x\neq 0\}\subset N$，且 $A\neq\varnothing\Rightarrow A$ 中必存在最小元，设为 $\delta(a)$，$\forall b\in I$，因 D 是欧氏环，故 $\exists g,r\in D$，使得

$$b=qa+r$$

且 $r=0$ 或 $\delta(r)<\delta(a)$，若为后者，因 $b\in I,qa\in I\Rightarrow r=b-qa\in I$，与 a 的取法矛盾，故 $r=0$，即 $b=qa\Rightarrow I=(a)$。

注意，本定理之逆不成立，因存在不是欧氏环的主理想整环。

类比整数环中最大公约数的定义，我们给出环中最大公约元的定义。

定义 3.5.6 设 R 是一个交换环，$a,b\in R$，称 $d\in R$ 是 a,b 的一个最大公约元，如果 d 满足：

(1) $d\mid a,d\mid b$；

(2) $\forall c\in R$，若 $c\mid a,c\mid b\Rightarrow c\mid d$。

将 a,b 的最大公约元 d 仍记做 $d=(a,b)$。

需要注意，任一整环的两个元 a,b，(a,b) 不一定存在，即使存在也不一定惟一，但由定义显然可得 a,b 的任意两个最大公约元一定相伴，且如果 $(a,b)=1$，称 a 与 b 互素。

定理 3.5.5 析因环 D 中任两元的最大公约元一定存在。

证 $\forall a,b\in D$，则

$$a=\varepsilon p_1^{k_1}p_2^{k_2}\cdots p_n^{k_n},b=\varepsilon' p_1^{l_1}p_2^{l_2}\cdots p_n^{l_n}$$

此处，ε,ε' 是单位，$p_1,p_2,\cdots,p_n$ 是不可约元，$k_i,l_i\in \mathrm{N}$，取 $m_i=\min(k_i,l_i)$，$i=1,2,\cdots,n$，则 $d=p_1^{m_1}p_2^{m_2}\cdots p_n^{m_n}=(a,b)$。

以上讨论了析因环的性质，但如何判定一个环是析因环，我们将给出一个判定定理，首先给出如下定义。

定义 3.5.7 设 R 是交换环。

R 有因子链条件 $\Leftrightarrow R$ 中不含无限的真因子序列；

R 有素性条件 $\Leftrightarrow R$ 中每个不可约元是素元；

R 有最大公约元条件 $\Leftrightarrow R$ 中任两元素都存在最大公约元。

定理 3.5.6 （析因环的判定定理）

整环 R 若满足因子链条件和素性条件，则 R 是析因环；整环 R 若满足因子链条件和最大公约条件，则 R 是析因环。

证明留做练习。

习题 3.5

1. 设 M 是析因的，证明：$ab\sim[a,b](a,b)$，$a,b\in M$。
2. 证明：$\mathbf{Z}[\sqrt{-5}]$满足因子链条件，并将 21 在 $\mathbf{Z}[-5]$中分解为不可约元素的乘积。
3. 证明：$\mathbf{Z}[x]$满足因子链条件。
4. 设 $D=\{a_1x^{\alpha_1}+a_2x^{\alpha_2}+\cdots+a_nx^{\alpha_n}\mid a_i$ 为域 F 的元，α_i 为非负有理数$\}$，用通常的方法定义相等和加法，用分配律和 $a_ix^{\alpha_i}\cdot a_jx^{\alpha_j}=a_ia_jx^{\alpha_i+\alpha_j}$ 定义乘法，证明：D 是整环，但 D 不满足因子链条件。
5. 设 $\mathbf{Z}[\sqrt{10}]=\{a+b\sqrt{10}\mid a,b\in\mathbf{Z}\}$，证明：$\mathbf{Z}[\sqrt{10}]$不是析因的。
6. 域 F 是主理想整环吗？
7. 设 $\mathbf{Z}[\sqrt{2}]=\{m+n\sqrt{2}\mid m,n\in\mathbf{Z}\}$，证明：$\mathbf{Z}[\sqrt{2}]$关于函数 $\delta(m+n\sqrt{2})=|m^2-2n^2|$是欧氏整环。
8. 设 $D=\{m+n\sqrt{-3}\mid m,n\in\mathbf{Z}$ 或 m,n 是奇整数的 $1/2\}$，证明：D 关于 $\delta(m+n\sqrt{-3})=m^2+3n^2$ 是欧氏整环。
9. 设 D 是主理想整环，E 是整环，且 D 是 E 的子环，d 是 a,b 在 D 中的最大公因子，则 d 也是 a,b 在 E 中的最大公约元。
10. 设 D 是主理想整环，$a\in D$ 且 $a\neq0$，若 a 是素数，则 $D/(a)$是域；若 a 不是素数，则 $D/(a)$不是整环。
11. 求出 $\mathbf{Z}[i]$的不可约元。
12. 设 a_1,a_2 是欧氏整环的非零元，通过 $a_1=q_1a_2+a_3$，$a_i=$

$q_i a_{i+1} + a_{i+2}$来定义 a_i, q_i，其中 $\delta(a_{i+2}) < \delta(a_{i+1})$，证明：存在 n，使得 $a_n \neq 0$，但 $a_{n+1} = 0$，且 $d = a_n = (a_1, a_2)$，因此 d 还可表示成形如 $xa_1 + ya_2$ 的表达式。

13. 通过下面规则来定义正整数的 Möbius 函数 $\mu(n)$：

(a) $\mu(1) = 1$；

(b) 如果 n 有一个平方因子，则 $\mu(n) = 0$；

(c) 如果 $n = p_1 p_2 \cdots p_s$，p_i 是不同的素数，则 $\mu(n) = (-1)^s$。

证明：

(ⅰ) 如果 $(n_1, n_2) = 1$，则 $\mu(n_1 n_2) = \mu(n_1)\mu(n_2)$。

(ⅱ) $\sum_{d \mid n} \mu(d) = \begin{cases} 1, & \text{如果 } n = 1; \\ 0, & \text{如果 } n \neq 1。\end{cases}$

14. 设 $\varphi(n)$ 是欧拉 φ 函数，证明：$\varphi(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) d$。

15. 设 z 是高斯整数环 $\mathbf{Z}[i]$ 的不可约元，证明：z 能且仅能整除一个素自然数。

§3.6 多项式环

我们首先给出多项式的形式表达定义。

定理 3.6.1 设 R 是交换环，令

$$R[x] = \{(a_0, a_1, \cdots) \mid a_i \in R, \text{只有有限个 } a_i \neq 0\}$$

定义

$$(a_0, a_1, \cdots) + (b_0, b_1, \cdots) = (a_0 + b_0, a_1 + b_1, \cdots)$$

$$(a_0, a_1, \cdots)(b_0, b_1, \cdots) = (c_0, c_1, \cdots)$$

其中

$$c_n = \sum_{i=0}^{n} a_{n-i} b_i = \sum_{k+j=n} a_k b_j$$

$$0 = (0, 0, \cdots)$$

$$1=(1,0,\cdots)$$

则$(R[x],+,\cdot,0,1)$是一个交换环。

证明是容易的，留做练习。

称定理3.6.1中的$R[x]$为R上的多项式环，其中的元素称为多项式。

目前，x在记号$R[x]$中是无意义的，但下面将构造出一个x，用它的出现去说明$R[x]$这个记号。注意到

$$\varphi:R\to R[x]$$
$$a\to a'=(a,0,\cdots)$$

是单同态，故a与a'视为等同，把R嵌入$R[x]$，把$(a,0,\cdots)$简记做a，则

$$a(a_0,a_1,\cdots)=(aa_0,aa_1,\cdots)$$

令$x=(0,1,0,\cdots)$，则$x^k=(0,0,\cdots,0,1,0,\cdots)$，其中1在第$k+1$个坐标，对$a\in R$，有

$$ax^k=(0,0,\cdots,0,a,0,\cdots)$$

其中a在第$k+1$个坐标，故

$$(a_0,a_1,\cdots,a_n,0,0,\cdots)=a_0+a_1x+\cdots+a_nx^n$$

称x为未定元，$R[x]$叫R上的未定元x的多项式环。可以证明

$$\sum a_ix^i=\sum b_ix^i\Leftrightarrow\forall i,a_i=b_i$$

$$\sum a_ix^i=0\Leftrightarrow\forall i,a_i=0$$

今后，环$R[x]$中的多项式$f(x)$记做形式表达式

$$f(x)=a_0+a_1x+\cdots+a_nx^n\quad(a_i\in R)$$

与许多代数结构一样，多项式环也可用泛映射性质来刻画，在环$R[x]$的定义的基础上，可研究任一添加元素u到R上的环$R[u]$，这可由下面的定理来描述。

定理3.6.2 设R与S是交换环，η是R到S的一个同态，$u\in S$，则存在惟一的映射$\eta_u:R[x]\to S$，η_u是同态，且η_u是η的扩

张，并且 $\eta_u(x)=u$。

证 设 $f(x)=\sum_{i=0}^{n}a_ix^i\in R[x]$，$g(x)=\sum_{i=0}^{m}b_ix^i\in R[x]$，则

$$f(x)g(x)=\sum_{i=0}^{n+m}c_ix^i,\ c_i=\sum_{j+k=i}a_jb_k$$

令

$$\eta_u(f(x))=\sum_{i=0}^{n}\eta(a_i)u^i$$

则

$$\eta_u(f(x)g(x))=\sum_{i=0}^{n+m}\eta(c_i)u^i$$

$$\eta(c_i)=\sum_{j+k=i}\eta(a_j)\eta(b_k)$$

而

$$\eta_u(f(x))\eta_u(g(x))=$$

$$(\sum_{i=0}^{n}\eta(a_i)u^i)(\sum_{i=0}^{m}\eta(b_i)u^i)=$$

$$\sum_{i=0}^{n+m}\eta(c_i)u^i$$

故

$$\eta_u(f(x)g(x))=\eta_u(f(x))\eta_u(g(x))$$

显然也有 $\eta_u(f(x)+g(x))=\eta_u(f(x))+\eta_u(g(x))$，且 $\eta_u(1)=\eta(1)=1_S$，故 η_u 是 $R[x]$ 到 S 的一个同态。

显然，$\eta_u(x)=u$，且 $\forall a\in R$，有

$$\eta_u(a)=\eta(a)$$

从而 η_u 是 η 的一个扩张。

又 $R[x]=\langle R,x\rangle$，由生成集上作用相同的映射必相等，故 η_u 是具有上述性质的惟一的同态。

推论 设 S 是 R 的扩环，$u\in S$，则存在 $R[x]$ 的一个理想 I，使 $R[u]\cong R[x]/I$，且 $I\cap R=\{0\}$；反之，若 $I\triangleleft R[x]$，使得 $I\cap R=\{0\}$，也有 $R[u]\cong R[x]/I$。

证 设 S 是 R 的扩环，$u\in S$，由定理 3.6.2，$\exists !$ 同态 η_u：$R[x]\to S$，$\eta_u|_R=1$，且 $\eta_u(x)=u$。

令 $f(x)=\sum_{i=0}^{n}a_ix^i\in R[x]$，则

$$\eta_u(f(x))=f(u)\in R[u]$$

令 $I=\ker\eta_u$，由同态基本定理，$R[u]\cong R[x]/I$，又 $\forall a\in R\cap I\Rightarrow\eta(a)=0$，且 $\eta(a)=a\Rightarrow a=0$，故 $R\cap I=\{0\}$。

反之，若 $I\triangleleft R[x]$，且 $I\cap R=\{0\}$，令

$$\gamma:R[x]\to R[x]/I$$

则 $\gamma|_R$ 是单同态，因由 $a_1,a_2\in R$，$a_1+I=a_2+I\Rightarrow a_1-a_2\in I$，且 $a_1-a_2\in R\Rightarrow a_1-a_2\in I\cap R=\{0\}\Rightarrow a_1=a_2$。

视 R 与 $\gamma(R)$ 等同，$a\in R$ 与 $a+I$ 等同，R 嵌入 $R[x]/I$ 视为它的一个子环，而 $R[x]=\langle R,x\rangle$，则 $\gamma(R[u])=\langle R,u\rangle$，其中 $u=x+I$，故

$$R[x]/I\cong R[u]$$

$\eta_u:f(x)\to f(u)$ 是单同态 $\Leftrightarrow\ker\eta_u=\{0\}\Leftrightarrow$ 若 $f(u)=0$，则 $f(x)=0\Leftrightarrow$ 由 $\sum_{i=0}^{n}a_iu^i=0$ 推出 $a_i=0$，$i=0,1,\cdots,n$，此时称 u 为 R 上的超越元，否则，称 u 为 R 上的代数元。

上面的讨论完全可以推广到任意有限多个未定元的情形。

定理 3.6.3 设 R,S 是交换环，η 是 R 到 S 的一个同态，$\forall n\in\mathbf{N}^*$，对由 $\{1,2,\cdots,n\}$ 到 S 的一个映射 $i\to u_i$ 来讲，存在惟一的由 $R[x_1,x_2,\cdots,x_n]$ 到 S 的同态 $\eta_{u_1u_2\cdots u_n}$，它是 η 的扩张，且 $\eta(x_i)=u_i$，$1\leqslant i\leqslant n$。

证 由归纳法易证,证明留给读者。

称 $R[x_1,x_2,\cdots,x_n]$为 R 上 n 个未定元 $x_1,x_2,\cdots,x_n$ 的多元多项式环。

上面的定理说明,对多元多项式环的构造,实质是逐次添加单个的未定元,而下面的定理保证了无论怎样添加,其结果是一样的。

定理 3.6.4 设 $\sigma\in S_n$,则在 $R[x_1,x_2,\cdots,x_n]$中存在惟一的自同构 $\zeta(\sigma)$,使得 $\zeta(\sigma)|_R=1$,且 $\zeta(\sigma)(x_i)=x_{\sigma(i)}$, $i=1,2,\cdots,n$。

证 设 S 为 R 的扩环,则由定理 3.6.3, 存在惟一的自同态 $\zeta(\sigma)$满足条件,往证 $\zeta(\sigma)$是自同构。

因 $R[x_1,x_2,\cdots,x_n]=\langle R\cup\{x_1,x_2,\cdots,x_n\}\rangle$,故若 $\sigma_1,\sigma_2\in S_n$,则 $\zeta(\sigma_1\sigma_2)=\zeta(\sigma_1)\zeta(\sigma_2)$,且 $\zeta(1)=1$。因此 $\zeta(1)=\zeta(\sigma\sigma^{-1})=\zeta(\sigma)\zeta(\sigma^{-1})=1\Rightarrow(\zeta(\sigma))^{-1}=\zeta(\sigma^{-1})$,故 $\zeta(\sigma)$是一个自同构。

若$(i_1,i_2,\cdots,i_n)\in N^{(n)}$,$(i_1,i_2,\cdots,i_n)\rightarrow x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$

$$R[x_1,x_2,\cdots,x_n]=\{\sum a_{i_1i_2\cdots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}\mid a_{i_1i_2\cdots i_n}\in R\}$$

与 $n=1$ 的情形相同,对任何一个环 $R[u_1,u_2,\cdots,u_n]$来说,$R[x_1,x_2,\cdots,x_n]$到 $R[u_1,u_2,\cdots,u_n]$的同态是同构$\Leftrightarrow\sum a_{i_1\cdots i_n}u_1^{i_1}\cdots u_n^{i_n}=0\Rightarrow a_{i_1\cdots i_n}=0$,此时称 n 个元素 $u_1,u_2,\cdots,u_n$ 为在R 上是代数无关的。

习题 3.6

1. 证明:

(i)复数 $\omega=-\frac{1}{2}+\frac{1}{2}\sqrt{3}i(i=\sqrt{-1})$在有理数域 Q 上是代数

元；

(ⅱ)设 I 是主理想(x^2+x+1)，$\mathbf{Q}[w]\cong\mathbf{Q}[x]/I$。

2. 证明：实数 $u=\sqrt{2}+\sqrt{3}$是代数元，并决定理想 I，使

$$\mathbf{Q}[u]\cong\mathbf{Q}[x]/I$$

3. 设 I 是 R 的理想，$I[x_1,x_2,\cdots,x_r]$是 $R[x_1,x_2,\cdots,x_r]$的子集且系数在 I 内，证明：$I[x_1,x_2,\cdots,x_r]$是环 $R[x_1,x_2,\cdots,x_r]$的理想。令 y_i 是 R/I 的不定元，证明：$R[x_1,x_2,\cdots,x_r]/I[x_1,x_2,\cdots,x_r]\cong(R/I)[y_1,y_2,\cdots,y_r]$。

4. 设 x_i 是未定元，证明：矩阵环 $M_n(R[x_1,x_2,\cdots,x_r])\cong M_n(R)[x_1,x_2,\cdots,x_r]$。

5. 设 $R[[x]]$为不受只有有限个 $a_i\neq 0$ 的限制序列$(a_0,a_1,\cdots)$的集合，其中 $a_i\in R$，如果像多项式环一样定义 $+$，$\cdot$，0，1，证明：从 $R[[x]]$可得到一个环，称这个环为有一个未定元的形式幂级数环。

§3.7　多项式环的因子分解

设 $R[x]$是交换环 R 上的一个未定元 x 的多项式环，$\forall f(x)\in R[x]$，则 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$，若 $a_n\neq 0$，称 a_n 为 $f(x)$的首项系数，而 n 叫 $f(x)$的次数，记做 $n=\deg f$，规定零多项式 0 的 $\deg 0=-\infty$，并规定 $\forall n\in\mathbf{Z}, n>-\infty$，$(-\infty)+n=-\infty=n+(-\infty)$，$(-\infty)+(-\infty)=-\infty$，并且定义

$$f(x)\in\mathbf{R}^*\Leftrightarrow\deg f=0$$

命题 3.7.1　若 $f(x)=\sum\limits_{i=0}^{n}a_ix^i$，$g(x)=\sum\limits_{j=0}^{m}b_jx^j$ 均属于 $R[x]$，则

$$\deg[f(x)+g(x)]\leqslant\max(\deg f(x),\deg g(x))$$

若等式成立⇔$\deg f=\deg g$。

$$\deg[f(x)g(x)]\leqslant \deg f(x)+\deg g(x)$$

此处要求 a_n 与 b_m 至少有一个不为零因子。显然，若 R 为整环，则等式成立。

证明是容易的，略。

定理 3.7.1 若 D 是整环，则 $D[x]$也是整环，且 $D[x]$的单位是 D 的单位。

证 若 $f(x)g(x)\in D[x]$，且 $f(x)g(x)=0\Rightarrow \deg fg=-\infty\Rightarrow \deg f=-\infty$或 $\deg g=-\infty\Rightarrow f(x)=0$ 或 $g(x)=0$。

若 $f(x)g(x)=1\Rightarrow \deg f=0=\deg g\Rightarrow f(x)\in D^*$，且 $f(x)$ 是 D 中的单位。

我们首先给出一个工具——除法算式，并导出重要的余数定理。

定理 3.7.2 （除法算式）

设 R 是交换环，$f(x),g(x)\in R[x]$，且 $g(x)\neq 0$，$g(x)=\sum_{i=0}^{m}b_ix^i$，$f(x)=\sum_{j=0}^{n}a_jx^j$，则 $\exists k\in \mathbf{N}$，$q(x),r(x)\in R[x]$，使得 $b_m^kf(x)=q(x)g(x)+r(x)$，并且 $\deg r<\deg q$。

证 若 $\deg f<\deg g$，由 $f(x)=0g(x)+f(x)$，结论成立。故设 $\deg f\geqslant \deg g$，令

$$b_mf(x)-a_nx^{n-m}g(x)=f_1(x)$$

因 $b_mf(x)$与 $a_nx^{n-m}g(x)$的首项系数均为 a_nb_m，故

$$\deg f_1<\deg f$$

由此可对 $f(x)$的次数用归纳法证明。

设对 $f_1(x)$，$\exists k-1\in \mathbf{N}$，$q_1(x),r(x)\in R[x]$，使得

$$b_m^{k-1}f_1(x)=g(x)q_1(x)+r(x)$$

则

$$b_m^k f(x) = b_m^{k-1}(b_m f(x)) =$$
$$b_m^{k-1}[a_n x^{n-m} g(x) + f_1(x)] =$$
$$b_m^{k-1} a_n x^{n-m} g(x) + g(x) q_1(x) + r(x) =$$
$$[b_m^{k-1} a_n x^{n-m} + q_1(u)] g(x) + r(x)$$

除法算式就是普通多项式的长除法，显然，若 b_m 是单位，得到 $f(x)=q(x)g(x)+r(x)$，且满足这样条件的 $q(x),r(x)$是惟一的。

推论 1 （余数定理）

若 $f(x)\in R[x], a\in R$，则存在惟一的 $q(x)\in R[x]$，使得

$$f(x) = (x-a)q(x) + f(a)$$

证 由定理 3.7.2 后面的说明，$\exists !\ q(x), r\in R[x]$，使得

$$f(x) = (x-a)q(x) + r$$

应用 φ 是 $R[x]$到 R 的同态，$\varphi|_R=1$，且 $\varphi(x)=a$，得

$$f(a) = (a-a)q(a) + r = r$$

推论 2 $(x-a)\mid f(u)\Leftrightarrow f(a)=0$

推论 3 若 F 是域，则 $F[x]$是欧氏环，从而是主理想整环和析因环。

证 由定理 3.7.1 知 $F[x]$是整环，令

$$\varphi: F[x]\setminus\{0\}\to \mathbf{N}$$
$$f(x)\to \deg f$$

由于域 F 中的非零元皆为单位，故取定 $g(x)\in F[x]\setminus\{0\}$，则 $\forall f(x)\in F[x]\setminus\{0\}$，$\exists !\ q(x), r(x)\in F[x]$，使

$$f(x) = g(x)q(x) + r(x)$$

且 $\deg r<\deg g$，从而 $F[x]$是欧氏环。

由于 $F[x]$中每个单位 f 的次数为 0，从而 f 是非零常数。

下面集中讨论析因环 D 上的多项式环 $D[x]$。

设 D 是析因环，则 D 的非零元素的任一有限集合都有最大

公约元，对 $a_i \in D, i=1,2,\cdots,n$，规定 $\forall a_i=0$，则 $(a_1,a_2,\cdots,a_n)=0$，当 a_i 不全为 0 时，$(a_1,a_2,\cdots,a_n)$ 为非零元 a_i 的最大公约元。

定义 3.7.1 设 $f(x)=\sum_{i=0}^{n} a_i x^i \in D[x]$，$D$ 为析因环，称 $f(x)$ 的所有系数的最大公约元 $(a_0,a_1,a_2,\cdots,a_n)$ 为 $f(x)$ 的容度，记做 $c(f)$，容度为 1 的多项式叫本原多项式。

本节的主要结论是下面这个定理。

定理 3.7.3 若 D 是析因环，则 $D[x]$ 也是析因环。

先证几个引理。

引理 1 (Gauss 引理)本原多项式的积是本原多项式。

证 设 $f(x), g(x)$ 是本原多项式，$f(x)=\sum_{i=0}^{n} a_i x^i$，$g(x)=\sum_{j=0}^{m} b_j x^j \Rightarrow f(x)g(x)=\sum_{k=0}^{m+n} c_k x^k$，其中 $c_k=\sum_{i+j=k} a_i b_j$，如果 $f(x)g(x)$ 非本原，则存在不可约元 $p\in D$，使得 $p\mid c_k(\forall k)$。

因 $c(f)=1\Rightarrow p\nmid c(f_1)\Rightarrow \exists s\in \mathbf{N}^*$，使得

$$p\mid a_i(\text{对 } i<s)\text{，但 } p\nmid a_s\text{。}$$

类似地，$\exists t\in\mathbf{N}^*$，使 $p\mid b_j$（对 $j<t$），但 $p\nmid b_t$，且 $p\mid c_{s+t}$，$c_{s+t}=a_0b_{s+t}+\cdots+a_{s-1}b_{t+1}+a_sb_t+a_{s+1}b_{t-1}+\cdots+a_{s+t}b_0\Rightarrow p\mid a_sb_t$，而 D 中的不可约元必为素元 $\Rightarrow p\mid a_s$ 或 $p\mid b_t$，此为矛盾，故 $f(x)\cdot g(x)$ 是本原多项式。

引理 2 设 F 是 D 的分式域，若 $D[x]$ 中的两个本原多项式 $f(x)$ 与 $g(x)$ 在 $F[x]$ 中相伴，则 $f(x)$ 与 $g(x)$ 在 $D[x]$ 中也相伴。

证 因 $F[x]$ 中的单位是 F 中的非零元，若 $f(x)$ 与 $g(x)$ 在 $F[x]$ 中相伴，$\exists 0\neq a\in F$，使 $f(x)=ag(x)$，令 $a=\frac{c}{b}$，$b,c\in D$，

$b\neq 0$，则 $bf(x)=cg(x)$，又 $c(f)=c(g)=1\Rightarrow c\mid b$ 且 $b\mid c\Rightarrow b$ 与 c 只相差 D 中的单位 ε，即 $c=b\varepsilon$，代入 $bf(x)=cg(x)\Rightarrow f(x)=\varepsilon g(x)$，即 $f(x)$ 与 $g(x)$ 在 $D[x]$ 中相伴。

引理 3 若 $f(x)\in D[x]$，$\deg f>0$，$f(x)$ 在 $D[x]$ 中是不可约的，则 $f(x)$ 在 $F[x]$ 中也不可约。

证 设 $f(x)$ 在 $F[x]$ 中是可约的 $\Rightarrow f(x)=\varphi_1(x)\varphi_2(x)$，其中 $\varphi_1(x),\varphi_2(x)\in F[x]$，且 $\deg\varphi_i(x)>0$，$i=1,2$，设 $\varphi_i(x)=a_if_i(x)$，$a_i\in F$，$f_i(x)$ 在 $D[x]$ 中是本原的，则

$$f(x)=a_1a_2f_1(x)f_2(x)$$

由引理 1，$f_1(x)f_2(x)$ 是本原的，由引理 2，$f(x)$ 与 $f_1(x)f_2(x)$ 在 $D[x]$ 中相伴，因 $\deg f_i(x)>0$，这与 $f(x)$ 在 $D[x]$ 中的不可约矛盾。

现证定理 3.7.3。

证 设 $f(x)\in D[x]$，$f(x)\neq 0$，$f(x)$ 不是单位，令 $f(x)=df_1(x)$，$d\in D$，$f_1(x)$ 是本原多项式，若 $f_1(x)$ 不是单位，且有真因子，则 $f_1(x)=f_{11}(x)f_{12}(x)$，$f_{1i}(x)(i=1,2)$ 既不是单位，又不是 D 中的元素，且

$$0<\deg f_{1i}<\deg f_1$$

继续下去，对 $f(x)$ 的次数用归纳法得

$$f_1(x)=q_1(x)q_2(x)\cdots q_t(x)$$

其中 $q_i(x)$ 在 $D[x]$ 中是不可约的。

若 d 不是单位，则

$$d=p_1p_2\cdots p_n$$

由此得到 $f(x)$ 的一种既约分解

$$f(x)=p_1p_2\cdots p_nq_1(x)q_2(x)\cdots q_t(x)$$

以下证这种分解是惟一的，即若 $f(x)$ 还有一种分解

$$f(x)=p_1'p_2'\cdots p_m'q_1'(x)q_2'(x)\cdots q_s'(x)$$

此处，$q_i'(x)$在 $D[x]$中不可约，且 $\deg q_i'>0$，则 $q_i(x)$，$q_i'(x)$ 均为本原多项式，由引理 1，$\prod\limits_{i=1}^{t} q_i(x)$，$\prod\limits_{j=1}^{s} q_j'(x)$ 均为本原多项式。

又因 $F[x]$是析因环，故$\prod\limits_{i=1}^{t} q_i(x) = \varepsilon \prod\limits_{j=1}^{s} q_j'(x) \Rightarrow t = s$，适当调换次序，有 $q_i(x) \sim q_i'(x)$，$i = 1,2,\cdots,t$。由引理 2，$q_i(x)$ 与 $q_i'(x)$ 在 $D[x]$ 中也相伴。又 D 是析因环，$\prod\limits_{i=1}^{n} p_i = \varepsilon' \prod\limits_{j=1}^{m} p_j' \Rightarrow m = n$，适当调换次序，$p_i \sim p_i'$。

故 $f(x)$的两种分解是相伴分解。

推论 若 D 是析因环，则 $D[x_1,x_2,\cdots,x_n]$也是析因环。

证 D 是析因环 $\Rightarrow D[x_1]$是析因环，而 $D[x_1,x_2] = D[x_1][x_2] \Rightarrow D[x_1,x_2]$ 也是析因环，由归纳法易证 $D[x_1,x_2,\cdots,x_n]$也是析因环。

习题 3.7

1. 设 F 是域，$f(x) = x^n + a_1x^{n-1} + \cdots + a_n$，其中 $a_i \in F$，$n>0$。令 $u = x + (f(x))$在 $F[x]/(f(x))$中，证明：

   (ⅰ)$F[u]$里的每个元素只能写成 $b_0 + b_1u + \cdots + b_{n-1}u^{n-1}$的形式，$b_j \in F$。

   (ⅱ)$F[u]$包含非零幂零元的充要条件是 $f(x)$具有平方因子，即 $f(x) = g^2(x)h(x)$，其中，$\deg(g(x))>0$。

2. 证明：

   (ⅰ)$x^3 + x^2 + 1$ 是$(\mathbf{Z}/(2))[x]$的不可约元。

   (ⅱ)$(\mathbf{Z}/(2))[x]/(x^2 + x + 1)$是具有 8 个元的域。

3. 构造具有 25 个元素的域及 125 个元素的域。

4. 证明：x^3-x 在 $\mathbf{Z}/(6)$中有 6 个根。

5. 证明：理想$(3,x^3-x^2+2x-1)$不是 $\mathbf{Z}[x]$的主理想，$\mathbf{Z}[x]/I$ 是整环吗？其中 $I=(3,x^3-x^2+2x-1)$。

6. 设 R 是环，且 R 没有不等于零的幂零元，即 $z^n=0\Rightarrow z=0$。如果 $f(x)$是 $R[x]$的零因子，证明：在 R 中存在不等于零的元素 a，使得 $af(x)=0$。

7. 设 F 是具有 q 个元素的域，$F^*=\{a_1,a_2,\cdots,a_{q-1}\}$是 F 的非零元集合，证明：$a_1a_2\cdots a_{q-1}=-1$。

8. 求 $\mathbf{Z}/(p)$的非零元的循环群 $\mathbf{Z}_p^*$ 的生成元，其中，$p=3,5,7$。

9. 设 $f(x),g(x)\neq 0$ 是 $F[x]$的元素，$\deg(g(x))=m$，证明：$f(x)$能惟一地写成表达式 $a_0(x)+a_1(x)g(x)+a_2(x)g(x)^2+\cdots+a_r(x)g(x)^r$，其中，$\deg a_i(x)<m$，$i=1,2,\cdots,r$。

10. 设 $f(x_1,x_2,\cdots,x_r)$是多项式，其系数属于一个无限域 F，如果能使另一个非零多项式 $g(x_1,x_2,\cdots,x_r)$的值 $g(c_1,c_2,\cdots,c_r)\neq 0$ 的所有$(c_1,c_2,\cdots,c_r)$都使 $f(c_1,c_2,\cdots,c_r)=0$，则 $f(x_1,x_2,\cdots,x_r)=0$。

11. 设 $f(x_1,x_2,\cdots,x_r)$满足 $f(0,0,\cdots,0)=0$ 和对每个$(a_1,a_2,\cdots,a_r)\neq(0,0,\cdots,0)$有 $f(a_1,a_2,\cdots,a_r)\neq 0$，如果 $g(x_1,x_2,\cdots,x_r)=1-f(x_1,x_2,\cdots,x_r)^{q-1}$，证明：

(ⅰ)$g(a_1,a_2,\cdots,a_r)=\begin{cases}1,(a_1,a_2,\cdots,a_r)=(0,0,\cdots,0)\\0,\text{其他。}\end{cases}$

(ⅱ)多项式 g 与 $f_0(x_1,x_2,\cdots,x_r)=(1-x_1^{q-1})(1-x_2^{q-1})\cdots(1-x_r^{q-1})$决定同一个多项式，则 $\deg g\geqslant r(q-1)$。

12. 证明阿廷－捷发莱(Artin-Chevalley)定理：$f(x_1,x_2,\cdots,x_r)$是 $n(n<r)$次多项式，并设 $f(0,0,\cdots,0)=0$，则有一个$(c_1,$

$c_2,\cdots,c_r)\neq(0,0,\cdots,0)$存在，使 $f(c_1,c_2,\cdots,c_r)=0$。

13. 令 F 是含有 q 个元素的一个有限域，证明：如果 $f(x_1,x_2,\cdots,x_r)$是一个非零多项式，对于每个 x_i 的次数都小于 q，则 F 里存在 c_i，使 $f(c_1,c_2,\cdots,c_r)\neq 0$。

14. 验证：$F[x_1,x_2,\cdots,x_r]$里任一个多项式可写成表达式 $\sum_{i=1}^{r} g_i(x_1,x_2,\cdots,x_r)(x_i^q-x_i)+g_0(x_1,x_2,\cdots,x_r)$，这里 g_0 对于每个 x_i 的次数都小于 q。

15. 证明：如果 $m(x_1,x_2,\cdots,x_r)$是一个多项式，使函数 $m(s_1,s_2,\cdots,s_r)=0$，则 $m(x_1,x_2,\cdots,x_r)$可写成表达式

$$\sum g_j(x_1,x_2,\cdots,x_r)(x_i^q-x_i)$$

16. 设 R 是析因整环，若 $f_1(x),f_2(x)\in R[x]$，$f_1(x)f_2(x)$是本原多项式，则 $f_1(x),f_2(x)$都是本原多项式。

17. 设 $f(x),g(x)\in R[x]$，$f(x)=af_1(x)$，$g(x)=bg_1(x)$，其中 $f_1(x)$，$g_1(x)$是本原多项式。如果 $g(x)\mid f(x)$，那么 $b\mid a$，$g_1(x)\mid f_1(x)$。

18. 设 $f_1(x),f_2(x),\cdots,f_n(x),\cdots$是 $R[x]$中本原多项式的序列，并且 $f_{i+1}(x)\mid f_i(x)$，$i=1,2,\cdots$。证明：这个序列只能有有限个互不相伴的项。

19. $f(x)$是 $\mathbf{Z}[x]$中首项系数为 1 的多项式，若 $f(x)$有有理根 α，则 α 是整数。

第 4 章　模

线性代数主要研究域上向量空间，模的概念[①]是向量空间概念的直接推广，只要用任意环代替域就得到这种推广。原因一方面是数学内部的逻辑结构促进了这样的推广工作；另一方面是线性变换 T 使 V 转化成 $F[\lambda]$上的模，得到了其他应用——有限 Abel 群的理论。

模的概念始于 1920 年，是德国女代数学家 E. Noether 首先提出来的，她在有限群的矩阵表示和代数结构这两个独立并行的体系中架起了桥梁。

本章主要研究主理想整环 D 上的模，它们分别给出有限生成 Abel 群的结构理论和线性变换的标准形。

§4.1　模的定义

设 M 是 Abel 加群，令

$$\text{End } M = \{\eta \mid \eta: M \to M, \eta(x+y) = \eta(x) + \eta(y), \eta(0) = 0\}$$

显然 $\eta(mx) = m\eta(x), \forall m \in \mathbf{Z}$，且由 Abel 加群的定义，$\eta(0) = 0$ 可以去掉。

在 End M 中规定

$$\eta\zeta(x) = \eta(\zeta(x))$$
$$(\eta + \zeta)(x) = \eta(x) + \zeta(x)$$

① 刘绍学. 近世代数基础. 北京：高等教育出版社，1999

$$1x = x$$
$$0x = 0, \forall x \in M$$
易证(End M, +, ·, 0, 1)是 Abel 加群 M 的自同态环。

设 R 是一个环,考虑同态映射

$$\eta: R \to \text{End } M$$
$$a \to \eta(a)$$

则对 $\forall x, y \in M$,有

$$\eta(a)(x + y) = \eta(a)(x) + \eta(a)(y)$$
$$\eta(a + b)(x) = (\eta(a) + \eta(b))(x) = \eta(a)(x) + \eta(b)(y)$$
$$\eta(ab)(x) = \eta(a) \cdot \eta(b)(x) = \eta(a)(\eta(b)(x))$$
$$\eta(1)(x) = x$$

设

$$\varphi: R \times M \to M$$
$$(a, x) \to \eta(a)(x) \triangleq ax$$

这就是环 R 到 M 上的作用,故有以下定义。

定义 4.1.1 设 R 是环,M 是 Abel 群,令 $\varphi:(a, x) \to ax$ 是 $R \times M$ 到 M 的一个映射,且满足:

(1) $a(x + y) = ax + ay$;

(2) $(a + b)x = ax + bx$;　　$(\forall x, y \in M, a, b, 1 \in R)$

(3) $(ab)x = a(bx)$;

(4) $1 \cdot x = x$。

称 M 是左 R-模。

类似地,利用

$$\varphi: M \times R \to M$$
$$(x, a) \to xa$$

可以定义右 R-模,从现在起,若不做特别说明,R-模均指的是左 R-模。容易看出,将所有关于左 R-模的定理加以必要的修改,均可适用于右 R-模,因左 R-模与右 R-模是对偶的。

例 1 每个 Abel 加群 M 是 $\mathbf{Z}$-模，这里，$na(n\in\mathbf{Z},a\in M)$像通常一样定义，故可将 Abel 群的理论包含在模的理论里。

例 2 设 R 是环，$S\leqslant R$，则 R 是 S-模，反之不对。但若 $S\triangle R$，则 S 是 R-模。特别地，0 和 R 均是 R-模，且 R/S 也是 R-模，其中 $a(b+S)=ab+S$。

例 3 设 R 是环，M 是 Abel 群，如果定义 $ax=0(\forall a\in R,x\in M)$，则 M 是平凡的 R-模。

设 R-模 M 的零元为 0_M，环 R 的零元为 0_R，容易证明，$a\cdot 0_M=0_M$，$0_R\cdot x=0_M$。今后将 0_R，0_M，$0\in\mathbf{Z}$ 及$\{0\}$均表示为 0，它的具体含义由它的上下文推知。

显然，$\forall a\in R,n\in\mathbf{Z},x\in M$，有

$$(-a)x=-(ax)=a(-x),n(ax)=a(nx)$$

由归纳法还知

$$a(\sum x_i)=\sum ax_i,(\sum a_i)x=\sum a_ix$$

定义 4.1.2 设 R 是环，M 是 R-模，$\varnothing\neq N\subset M$，称 N 是 M 的子模，是指 N 是 M 的子加群，且 $\forall a\in R,y\in N\Rightarrow ay\in N$。

例 4 M 是 $\mathbf{Z}$-模，M 的子模是$(M,+,0)$的子加群。

例 5 V 是域 F 上的向量空间，V 的子模是 V 的子空间。

例 6 如果$\{N_\alpha\mid\alpha\in\mathscr{A}\}$是模 M 的子模族，则 $\bigcap\limits_{\alpha\in\mathscr{A}}$ 也是 M 的子模。

例 7 设 M 是 R-模，若 $0\neq S\subset M$，则$\langle S\rangle$是 M 的子模，且

$$\langle S\rangle=\{\sum_{i=1}^{r}a_iy_i\mid a_i\in R,y_i\in S\}$$

若$|S|<\infty$，则称$\langle S\rangle$为有限生成模，若$|S|=1$，即 $S=\{a\}$，称$\langle S\rangle$为 a 生成的循环子模。

例 8 设$\{N_\alpha\mid\alpha\in\mathscr{A}\}$为 M 的子模族，则

$$\langle\bigcup_{\alpha\in\mathscr{A}}N_\alpha\rangle=\{y_{\alpha_1}+y_{\alpha_2}+\cdots+y_{\alpha_r}\mid y_{\alpha_k}\in N_{\alpha_k},k=1,2,\cdots,r\}$$

称为由 N_α 生成的子模,记做 $\sum N_\alpha$ 。

若 $\{N_\alpha\}=\{N_1,N_2,\cdots,N_m\}$,则

$$\langle\bigcup_{i=1}^{m}N_i\rangle = \sum_{i=1}^{m}N_i = N_1 + N_2 + \cdots + N_m$$

为了方便,N 是 M 的子模仍采用记号 $N\leqslant M$。

定义 4.1.3 设 N 是 R-模 M 的子模,令

$$\overline{M} = M/N = \{\bar{x} = x + N \mid x \in M\}$$

定义

$$(x_1 + N) + (x_2 + N) = x_1 + x_2 + N$$

$$a\bar{x} = a(x + N) = ax + N = \overline{ax}$$

易证这样定义的运算与代表元的选取无关,且满足模定义中的 4 条,称 $\overline{M}=M/N$ 是 R-商模。

当且仅当相关联的环相同时才有模同态的定义。

定义 4.1.4 设 M 和 M' 都是 R-模,称

$$\eta: M \rightarrow M'$$

为 R-模同态,如果满足:

(1) $\eta(x+y)=\eta(x)+\eta(y),\eta(0)=0$;

(2) $\eta(ax)=a\eta(x),\forall a\in R,\forall x,y\in M$。

同样,由 η 的单射、满射和双射分别有模单同态、模满同态及模同构的概念。

显然,$\ker\eta=\eta^{-1}(0)=\{y\mid\eta(y)=0,y\in M\}\leqslant M$。(只需注意 $\eta(ay)=a\eta(y)=0$ 即可)

$\eta(M)=\{\eta(x)\mid x\in M\}\leqslant M'$。(因若 $y\in\eta(M),ay=a\eta(x)=\eta(ax)\in\eta(M)$)

从上述定义,可以联想到,关于群的同态基本定理及各种同构定理,经过必要的修改,对模也成立。在证明的每一步中,只需确认每个子群是子模,群同态是模同态即可。这里不加证明,罗列其

后。

定理 4.1.1 设 N 是 R-模 M 的子模，η 是 M 到 M' 的模同态，且 $N \subseteq \ker \eta$，则存在惟一的

$$\begin{aligned} \bar{\eta}: M/N &\to M' \\ \bar{x} &\to \eta(x) \end{aligned}$$

是模同态，使得 $\eta = \bar{\eta} \cdot \gamma$，其中 $\gamma: M \to \overline{M}$ 是自然模同态，并且 $\bar{\eta}$ 是单同态当且仅当 $N = \ker \eta$。

定理 4.1.2 若 η 是 M 到 M' 的模同态，则

$$M/\ker \eta \cong \eta(M)$$

定理 4.1.3 若 N 和 N' 是 R-模 M 的子模，则

$$N/(N \cap N') \cong (N + N')/N'$$

定理 4.1.4 若 N 和 N' 是 R-模 M 的子模，且 $N' \subset N$，则

$$N/N' \leqslant M/N'$$

$$M/N' \big/ N/N' \cong M/N$$

循环模 $M = \langle x \rangle$ 记做 $M = Rx = \{ax \mid a \in R, x \in M\}$。

视 R 为自身 R 上的模，令

$$\begin{aligned} \mu_x: R &\to Rx \\ a &\to ax \end{aligned}$$

显然，μ_x 是加群 $(R, +, 0)$ 的同态，且

$$\mu_x(ba) = (ba)x = b(ax) = b\mu_x(a)$$

故 μ_x 是 R 的模同态，且是模满同态，故

$$M = Rx \cong R/\ker \mu_x$$

而 $\ker \mu_x = \{d \in R \mid ax = 0\}$ 是 R 的子模，将它视为环时，它是 R 的左理想，称它为 x 的左零化子，记做 $\operatorname{ann} x$，故

$$Rx \cong R/\operatorname{ann} x$$

且若 $\operatorname{ann} x = 0 \Rightarrow Rx \cong R$。

特别地，$R = \mathbf{Z} \Rightarrow \mathbf{Z}x \cong R$ 或 $\operatorname{ann} x = (n)$，$n > 0$，$n$ 是使 $nx = 0$

的最小正整数，显然 $n=|\langle x\rangle|$，称 ann x 为 x 的阶理想。

最后指出，与 Abel 群 M 的自同态环 End M 一样，由模 M 到模 M 的所有模同态构成的集合

$$\mathrm{Hom}\,(M,M)=\{\eta\mid\eta\text{是}M\text{到}M\text{的模同态}\}$$

也是一个环，称为模 M 的自同态环，记做 $\mathrm{End}_R M$。

证明仅比 End M 的证明多一个步骤，留给读者。

习题 4.1

1. 确定 Aut M，其中 $M=(\mathbf{Z}^{(2)},+,0)$。
2. 确定 $\mathrm{End}(\mathbf{Q},+,0)$。
3. 设 M 为左 R-模，η 是环 S 到环 R 的同态，证明：若定义 $ax=\eta(a)x$，$a\in S$，$x\in M$，则 M 是左 S-模。
4. 设 M 为左 R-模，$B=\{b\in R,bx=0,\forall x\in M\}$，验证 B 是 R 的理想。并证明若 C 是含在 B 中的 R 的理想，规定 $(a+C)x=ax$，则 M 是左 R/C-模。
5. 设 M 是左 R-模，S 是 R 的子环，若规定 $bx(b\in S,x\in M)$ 和 M 作为左 R-模时作用相同，证明：M 是左 S-模，特别地，环 R 是左 S-模。
6. 设 $V=\mathbf{R}^{(n)}$ 是实 n 元数组构成的向量空间，T 是 V 的线性变换：$x=(x_1,x_2,\cdots,x_n)\to Tx=(x_n,x_1,\cdots,x_{n-1})$，将 V 作为左 $R[\lambda]$-模，试确定：

   (i) λx；

   (ii) $(\lambda^2+2)x$；

   (iii) $(\lambda^{n-1}+\lambda^{n-2}+\cdots+1)x$。

   (iv) 什么样的元素能满足 $(\lambda^2-1)x=0$？
7. 同上题，设 B 是如第 4 题那样确定的 $R[\lambda]$ 的理想，试给出 B 的明显表达式。

8. 设 M 是加群,证明有且仅有一种方法使 M 成为左 $\mathbf{Z}$-模。

9. 设 M 是左 $\mathbf{Q}$-模,证明:所给定的 $\mathbf{Q}$ 的作用是使 M 为左 $\mathbf{Q}$-模的惟一方法。

10. 设 $M\neq 0$ 是有限 Abel 群,M 能否成为左 $\mathbf{Q}$-模?

11. 确定 $\mathrm{Hom}[\mathbf{Z},\mathbf{Z}/(n)]$,$\mathrm{Hom}[\mathbf{Z}/(n),\mathbf{Z}]$,其中 $n>0$,$\mathbf{Z}$ 和$\mathbf{Z}/(n)$ 均为 $\mathbf{Z}$-模。

12. 证明:$\mathrm{Hom}[\mathbf{Z}^{(2)},\mathbf{Z}]\cong[\mathbf{Z}^{(2)},+,0]$。

13. 证明:对任意的环 R 及 R-模 M 有

$$\mathrm{Hom}(R,M)\cong(M,+,0)$$

14. 在 $\mathrm{End}\,M$ 中,证明 $\mathrm{End}_R\,M$ 是自同态 $a_L(a\in R)$的集合之中心化子。

15. 判断 $a_L\in\mathrm{End}_R\,M$ 是否正确。

16. 如果 $M\neq 0$,且 M 只有 0 和 M 这两个子模,则称 M 为不可约的。证明:M 是不可约的充要条件是 $M\neq 0$,且 M 的每个非零元都是循环模的生成元。

17. 设 I 是 R 的左(右)理想,如果 $R\neq I$ 且没有左(右)理想 I' 使 $R\supsetneqq I'\supsetneqq I$,则称 I 是 R 的极大左(右)理想。证明:R-模 M 是不可约的充要条件为 $M\cong R/I$,其中 I 是 R 的极大左理想。

18. (Schur 引理)证明:若 M_1,M_2 是不可约模,则 M_1 到 M_2 的任何一个非零的同态是同构,进而证明若 M 是不可约的,则 $\mathrm{End}_R\,M$ 是除环。

19. 上题的逆是否成立?即 $\mathrm{End}_R\,M$ 是除环,则 M 一定是不可约的吗?

20. 如果 I 是 A 的一个左理想,令 IM 表示有限和 $\sum b_ix_i$ 的集合,这里 $b_i\in I,x_i\in M$,证明:IM 是 M 的一个子模。

21. 如果 I 是 A 的一个右理想,对 $\forall b\in I$,证明:能使 $by=0$ 的元素 $y(y\in M)$的全体是一个子模。

§4.2 自由模

与群的直积类似,这里首先给出模的直和的定义。

定义 4.2.1 设 $M_i, i=1,2,\cdots,n$ 是同一个环 R 上的模,令

$$M = \prod_{i=1}^{n} M_i = \{(x_1, x_2, \cdots, x_n) \mid x_i \in M_i, i = 1,2,\cdots,n\}$$

定义

$$(x_1, x_2, \cdots, x_n) + (y_1, y_2, \cdots, y_n) =$$
$$(x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n)$$
$$0 = (0,0,\cdots,0)$$
$$a(x_1, x_2, \cdots, x_n) = (ax_1, ax_2, \cdots, ax_n), a \in R$$

称 M 为 M_i 的直和,记为 $M_1 \oplus M_2 \oplus \cdots \oplus M_n \triangleq \oplus M_i$。

设 η_i 是 M_i 到模 N 的同态,$i=1,2,\cdots,n$,则

$$\eta: \oplus M_i \to N$$

$$(x_1, x_2, \cdots, x_n) \mapsto \sum_{i=1}^{n} \eta_i(x_i)$$

是 $\oplus M_i$ 到 N 的同态。

定理 4.2.1 令 M 是 R-模,且 $M_i \leqslant M, i=1,2,\cdots,n$,具有性质:

(1) $M = M_1 + M_2 + \cdots + M_n$;

(2) $\forall i=1,2,\cdots,n$,有

$$M_i \cap (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_n) = 0$$

则 $\oplus M_i \cong M$。

反之,在 $\oplus M_i$ 中,令

$$M_i' = \{(0,0,\cdots,x_i,0,\cdots,0) \mid x_i \in M_i\}$$

则 $M_i' \leqslant \oplus M_i$,且 $M_i' \cong M_i$,对 M_i' 条件(1),(2)成立。

证 取 $\eta_i = 1 : x_i \to x_i$，则

$$\eta : \bigoplus M_i \to M$$

$$(x_1, x_2, \cdots, x_n) \mapsto \sum_{i=1}^{n} x_i$$

是同态映射。

$\forall x \in M, x = \sum_{i=1}^{n} x_i, x_i \in M_i$，由条件(1)，$\exists (x_1, x_2, \cdots, x_n) \in \bigoplus M_i$，使得 $\eta(x_1, x_2, \cdots, x_n) = \sum_{i=1}^{n} x_i = x$，故 η 是满射。

若 $\sum_{i=1}^{n} x_i = 0 \Rightarrow -x_i = \sum_{j \neq i} x_j \Rightarrow x_i \in M_i \in M_i \cap (\sum_{i \neq j} M_j) = 0 \Rightarrow x_i = 0 \Rightarrow x = 0$ 即 $\ker \eta = 0$。

故 η 是同构，即$\bigoplus M_i \cong M$。

反之，设

$$\Gamma_i : M_i \to M$$

$$x_i \to (0, \cdots, 0, x_i, 0, \cdots, 0)$$

是单同态，$\Gamma_i(M_i) = M_i' \leqslant M, M_i \cong M_i'$。

在 M_i'中，由$(x_1, 0, \cdots, 0) + (0, x_2, 0, \cdots, 0) + \cdots + (0, 0, \cdots, x_n) = (x_1, x_2, \cdots, x_n)$，故条件(1)成立，而 $\sum_{j \neq i} M_j' = \{(x_1, \cdots, x_{i-1}, 0, x_{i+1}, \cdots, x_n\}$，显然有

$$M_i \cap \sum_{j \neq i} M_j = 0$$

本定理定义的直和称为内直和，定义 4.2.1 中的直和叫外直和。由于内直和与外直和等同，统一记做$\bigoplus M_i$。

若子模族$\{M_i\}$满足条件(2)，则称$\{M_i\}$是无关的。显然，$\{M_i\}$无关$\Leftrightarrow \sum_{i=1}^{n} x_i = 0, x_i \in M_i \Leftrightarrow x_i = 0, i = 1, 2, \cdots, n$。

$\{M_i\}$无关$\Leftrightarrow \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} y_i \Leftrightarrow x_i = y_i, i = 1,2,\cdots,n$。可以看出，无关条件强于 $M_i \cap M_j = 0, i \neq j$，也强于 $M_i \cap (\bigcup_{j\neq i} M_i) = 0$。

与向量空间的直和分解雷同，有下面的定理。

定理 4.2.2 设 $M = \oplus M_i, M_i \leqslant M$，令 $N_1 = \sum_{i=1}^{r_1} M_i, N_2 = \sum_{i=r_1+1}^{r_1+r_2} M_i, \cdots$，则 $M = \oplus N_j$；也有，若 $M_i = \oplus M_{ij}, 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n$，则

$$M = \oplus M_{ij}$$

证明留给读者。

在模的直和定义中，视环 R 为 R-模，则 $R \oplus R \oplus \cdots \oplus R \triangleq R^{(n)} = \{(x_1, x_2, \cdots, x_n) \mid x_i \in R, i = 1,2,\cdots,n\}$是 R-模。

令 $e_i = (0,\cdots,0,1,0,\cdots,0), i = 1,2,\cdots,n$，其中 1 在第 i 个坐标位置上。

$\forall x \in R^{(n)}$，则 $x = \sum_{i=1}^{n} x_i e_i$，故 $R^{(n)} = \langle e_1, e_2, \cdots, e_n \rangle$，且若

$$\sum_{i=1}^{n} x_i e_i = 0 \Rightarrow x_i = 0, \forall i (1 \leqslant i \leqslant n)$$

称 $e_1, e_2, \cdots, e_n$ 为 $R^{(n)}$ 的基。

设 M 是任一 R-模，$u_1, u_2, \cdots, u_n$ 是 M 的基，即：

(1) $M = \langle u_1, u_2, \cdots, u_n \rangle$；

(2) 若 $\sum_{i=1}^{n} a_i u_i = 0 \Rightarrow a_i = 0, \forall i = 1,2,\cdots,n$。

则存在由 $R^{(n)}$ 到 M 的惟一的同态映射

$$\mu: R^{(n)} \to M$$
$$\sum a_i e_i \to \sum a_i u_i$$

使得 $\mu(e_i)=u_i, i=1,2,\cdots,n$。

显然，$\text{im}\ \mu \leqslant M$，而 $\text{im}\ \mu \supset \{u_1,u_2,\cdots,u_n\} \Rightarrow \text{im}\ \mu = M$。

此外，若 $x=(x_1,x_2,\cdots,x_n)\in \ker \mu \Rightarrow \sum x_i u_i = 0 \Rightarrow x_i = 0$，$i=1,2,\cdots,n \Rightarrow x=0 \Rightarrow \ker \mu = 0$。

故 μ 是同构，即 $M\cong R^{(n)}$，称 M 是秩为 n 的 R-自由模。

自由模的基不一定惟一，但若是可换环 R 上的自由模，则基的个数是惟一的。

定理 4.2.3 若 M 是可换环 R 上的模，且 M 有 m 个元和 n 个元的基，则 $m=n$。

证 设 $\{e_i \mid 1\leqslant i\leqslant n\}$，$\{f_j \mid 1\leqslant j\leqslant m\}$ 是 M 的基，则有

$$f_j = \sum_{i=1}^{n} a_{ji} e_i$$

$$e_i = \sum_{j=1}^{m} b_{ij} f_j$$

故

$$f_j = \sum_{i=1}^{n}\sum_{k=1}^{m} a_{ji} b_{ik} f_k$$

$$e_i = \sum_{j=1}^{m}\sum_{l=1}^{n} b_{ij} a_{jl} e_l$$

因 $\{e_i\}$，$\{f_j\}$ 是基，有

$$\sum_{i=1}^{n} a_{ji} b_{ik} = \begin{cases} 1, j = k \\ 0, j \neq k \end{cases} \quad ①$$

$$\sum_{j=1}^{m} b_{ij} a_{jl} = \begin{cases} 1, i = l \\ 0, i \neq l \end{cases} \quad ②$$

设 $m<n$，令

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}_{n \times n}$$

$$B = \begin{pmatrix} b_{11} & \cdots & b_{1m} & 0 & \cdots & 0 \\ b_{21} & & b_{2m} & 0 & \cdots & 0 \\ \vdots & & & & & \vdots \\ b_{n1} & \cdots & b_{nm} & 0 & \cdots & 0 \end{pmatrix}_{n \times n}$$

由②式及 $m < n$ 得，$\boldsymbol{BA} = \boldsymbol{I}$，而 R 是可换环，故 $AB = I$，但 AB 的后 $n - m$ 行是 0，故 $\boldsymbol{AB} \neq \boldsymbol{I}$，此为矛盾，因此 $m \geqslant n$。由对称性，$n \geqslant m \Rightarrow m = n$。

推论 1 设 R 为交换环，则 $R^{(m)} \cong R^{(n)} \Rightarrow m = n$。

推论 2 设 $\{e_i\}$，$\{f_i\}$ 是 R-自由模 M 的基，且 $f_j = \sum_{i=1}^{n} a_{ji} e_i$，$e_i = \sum_{j=1}^{n} b_{ij} f_j$，其中 $\boldsymbol{A} = (a_{ij})$，$\boldsymbol{B} = (b_{ij})$，则 $\boldsymbol{AB} = \boldsymbol{BA} = \boldsymbol{I}$，即 $\boldsymbol{A}$，$\boldsymbol{B} \in L_n(R)$。

当 R 为非可换环时，向量空间的许多原则在自由模中也是适用的。例如，任一线性变换 σ 与在一组基下的矩阵 $\boldsymbol{A}$ 之间存在一一对应，这个原则在自由模中可推广为以下定理。

定理 4.2.4 设 $\{e_i \mid 1 \leqslant i \leqslant n\}$，$\{f_j \mid 1 \leqslant j \leqslant m\}$ 是 R-自由模 M 的基，设

$$\mathrm{Hom}(R^{(m)}, R^{(n)}) = \{\eta \mid \eta \text{ 是 } R^{(m)} \text{ 到 } R^{(n)} \text{ 的同态}\}$$

$$M_{m,n}(R) = \{(a_{ij})_{m \times n} \mid a_{ij} \in R\}$$

则

$$\mathrm{Hom}(R^{(m)}, R^{(n)}) \cong M_{m,n}(R)$$

证　设 $\eta(e_i)=\sum_{j=1}^{n}a_{ij}f_j,i=1,2,\cdots,m$，称 $\mathbf{A}=(a_{ij})_{m\times n}$ 为 η 关于基 $(e_1,e_2,\cdots,e_m),(f_1,f_2,\cdots,f_n)$ 的矩阵，则 η 由 $\mathbf{A}$ 所确定，这是因为若 $x=(x_1,x_2,\cdots,x_m)=\sum_{i=1}^{m}x_ie_i$，则

$$\eta(x)=\eta(\sum_{i=1}^{m}x_ie_i)=\sum_{i=1}^{m}x_i\eta(e_i)=\sum_{i=1}^{m}\sum_{j=1}^{n}x_ia_{ij}f_j$$

故 η 是映射

$$(x_1,x_2,\cdots,x_m)\to(y_1,y_2,\cdots,y_n)$$

其中 $y_j=\sum_{i=1}^{m}x_ia_{ij},j=1,2,\cdots,n$，因此 η 由 $\mathbf{A}$ 所确定，令

$$\varphi:\mathrm{Hom}(R^{(m)},R^{(n)})\to M_{m,n}(R)$$
$$\eta\to\mathbf{A}$$

由上面的讨论知 φ 是映射，且显然是满单射，并有

$$\varphi(\eta+\zeta)=\varphi(\eta)+\varphi(\zeta)$$
$$\varphi(\eta\zeta)=\varphi(\eta)\varphi(\zeta)$$
$$\varphi(0)=0$$
$$\varphi(1)=1$$

故

$$\mathrm{Hom}(R^{(m)},R^{(n)})\cong M_{m,n}(R)$$

习题 4.2

1. 设 R 是任意一个环，$(e_1,e_2,\cdots,e_n)$ 是 $R^{(n)}$ 的基，证明：$(f_1,f_2,\cdots,f_m)$（$f_j=\sum_{i=1}^{n}a_{ji}e_i$）是 $R^{(m)}$ 的基的充要条件是存在 $n\times m$ 型矩阵 $\boldsymbol{B}$，使得 $\boldsymbol{AB}=\boldsymbol{I}_m,\boldsymbol{BA}=\boldsymbol{I}_n$，其中 $\boldsymbol{A}=(a_{ij}),\boldsymbol{I}_m,\boldsymbol{I}_n$ 分别为 $m\times m,n\times n$ 型单位矩阵。从而证明 $R^{(m)}\cong R^{(n)}$ 的充要

条件是存在 $A\in N_{m,n}(R)$ 及 $B\in M_{n,m}(R)$，使 $AB=I_m$，$BA=I_n$。

2. 设 $\eta\in \mathrm{End}_R(R^{(n)})$，$A$ 是 η 关于基$(e_1,e_2,\cdots,e_n)$的矩阵，令 $f_i=\sum\limits_{j=1}^{n}p_{ij}e_j$，其中 $P=(p_{ij})\in L_n(R)$，验证 η 关于基$(f_1,\cdots,f_n)$的矩阵为 PAP^{-1}。

3. 用 R_n 表示具有基 $e_1,e_2,\cdots,e_n$ 的自由模，设 $\eta\in\mathrm{End}_R R_n$，$\eta(e_i)=\sum\limits_{j=1}^{n}e_ja_{ji}$，证明：$\eta\to A=(a_{ij})$是 $\mathrm{End}_R R_n$ 到 $M_n(R)$上的同构。

4. 设 R 是交换环，证明：如果 η 是$R^{(n)}$的满自同态，则 η 是双射，如果 η 是单自同态，是否有这样的结论呢？

5. 设 R 是可换环，M,N 是 R-模，如果 $a\in R$，$\eta\in\mathrm{Hom}(M,N)$，规定 $a\eta$ 为$(a\eta)(x)=a(\eta x)=\eta(ax)$，证明：$a\eta\in\mathrm{Hom}(M,N)$，且 $\mathrm{Hom}(M,N)$是 R-模，并证明 $\mathrm{Hom}(R^{(m)},R^{(n)})$是秩为 mn 的自由模。

6. 设 R 是交换整环，$(e_1,e_2,\cdots,e_n)$是 $R^{(n)}$ 的一组基，令 $f_i=\sum\limits_{j=1}^{n}a_{ij}e_j$，其中 $A=(a_{ij})\in M_n(R)$，证明：

(ⅰ)这些 f_i 构成$R^{(n)}$的自由子模 K 的基当且仅当 $\det A\neq 0$；

(ⅱ)对任意的 $\bar{x}=x+K\in R^{(m)}/K$，有等式$(\det A)\bar{x}=0$。

7. 设 V 是域F 上的向量空间，证明：V 的非零向量组 $x_i(1\leqslant i\leqslant n)$是线性无关的，当且仅当这些子空间 Fx_i 是无关的，并证明这些 x_i 构成基当且仅当 $V=\oplus Fx_i$。

8. 设 M 是模，$M_i(1\leqslant i\leqslant n)$是 M 的子模，使得

$$M=\sum M_i$$

$$M_1\cap M_2=0$$

$$(M_1 + M_2) \cap M_3 = 0$$

$$\vdots$$

$$(M_1 + M_2 + \cdots + M_{n-1}) \cap M_n = 0$$

证明：$M = \bigoplus M_i$。

9. 证明：设 p 为素数，$e \in \mathbf{Z}$ 且 $e > 0$，将 $\mathbf{Z}/(p^e)$ 看成 $\mathbf{Z}$-模，它不是两个非零子模的直和。对于 $\mathbf{Z}$ 有这样的结论成立吗？对于其他正整数 n，$\mathbf{Z}/(n)$ 有这样的结论成立吗？

10. 证明：若 $M = M_1 \oplus M_2$，则 $M_1 \cong M/M_2$，$M_2 \cong M/M_1$。

§4.3　主理想整环上的模

设 D 是主理想整环，本节主要研究主理想整环上的有限生成模，即 M 是 D 上的模，且 $M = \langle x_1, x_2, \cdots, x_n \rangle$，即 $M = \sum\limits_{i=1}^{n} Dx_i$。

一般地，自由模的子模不一定是自由模，但主理想整环上的自由模的子模一定是自由模，这就是下面的定理。

定理 4.3.1　设 $D^{(n)}$ 是主理想整环 D 上秩为 n 的自由模，则 $D^{(n)}$ 的任一子模 K 也是自由模，且 K 的秩 $m \leqslant n$。

证　若 $K = 0$，规定仅有零元组成的模是零秩自由模。而当 $n = 0$ 时，定理是显然成立的。

下面对 n 用归纳法证明。

(1)设 $n = 1$，则 $D^{(1)} = D$，若 K 是 D 的子模，则 K 是环 D 的理想 $\Rightarrow K = (f)$（因 D 是主理想），若 $f = 0$，则 $K = 0$，否则 $f \neq 0$，由 $af = 0 \Rightarrow a = 0$（因 D 是整环），故 K 是以 f 为基的自由模。

(2)设 $n-1$ 时，结论成立。

令 $\{e_i \mid 1 \leqslant i \leqslant n\}$ 是 $D^{(n)}$ 的基，并设

$$D^{(n-1)} = \langle e_2, e_3, \cdots, e_n \rangle$$

则 $D^{(n-1)}$是秩为 $n-1$ 的自由模，而 $D^{(n)}/D^{(n-1)}$是基为$\overline{e_1}=e_1+D^{(n-1)}$的自由模，且

$$\overline{K}=(K+D^{(n-1)})/D^{(n-1)}\leqslant\overline{D^{(n)}}=D^{(n)}/D^{(n-1)}$$

若 $\overline{K}=0\Rightarrow K+D^{(n-1)}=D^{(n-1)}\Rightarrow K\subset D^{(n-1)}$，由归纳法，定理得证。

若 $\overline{K}\neq 0$，由 $n=1$ 的证明结果得

$$\overline{K}\text{ 有基}\overline{f_1}=f_1+D^{(n-1)}\Rightarrow f_1\in K$$

再将归纳法假设用于 $K\cap D^{(n-1)}$，它是 $D^{(n-1)}$ 的子模。若 $K\cap D^{(n-1)}\neq 0$，由归纳法假设

$$K\cap D^{(n-1)}\text{ 有基}(f_2,\cdots,f_m),0<m-1\leqslant n-1$$

今断言，$(f_1,f_2,\cdots,f_m)$就是 K 的基。证明如下：

首先，设 $y\in K\Rightarrow\bar{y}=y+D^{(n-1)}\in\overline{K}\Rightarrow\bar{y}=b_1\overline{f_1},b_1\in D\Rightarrow y-b_1f_1\in D^{(n-1)}$，取 $f_1\in K\Rightarrow y-b_1f_1\in K\Rightarrow y-b_1f_1\in K\cap D^{(n-1)}\Rightarrow y-b_1f_1=\sum_{i=2}^{m}b_if_i\Rightarrow y=\sum_{i=1}^{m}b_if_i$。

其次，设 $\sum_{j=1}^{m}b_jf_j=0\Rightarrow b_1\overline{f_1}=-\sum_{k=2}^{m}b_k\overline{f_k}=0$，由$\overline{f_1}$是$\overline{D^{(n)}}$的基$\Rightarrow b_1=0$，再由 $k\geqslant 2$ 时，f_k 是$K\cap D^{(n-1)}$ 的基$\Rightarrow\sum_{k=2}^{m}b_kf_k=0\Rightarrow b_k=0$。

故$(f_1,f_2,\cdots,f_m)$是 K 的基。

若 $K\cap D^{(n-1)}=0$，同样可证 f_1 是 K 的基。

特别地，域 F 是主理想整环，而域上的模就是向量空间，可得出线性代数熟知的定理。

下面讨论子模 K 的基未知但K 是有限生成的情形，即

$$K=\langle f_1,f_2,\cdots,f_m\rangle$$

此处，m 可能大于n，则

$$f_i = \sum_{j=1}^{n} a_{ij} e_j, i = 1,2,\cdots,m$$

称 $\boldsymbol{A}=(a_{ij})_{m\times n}$ 为 $(f_1,f_2,\cdots,f_m)$ 在有序基 $(e_1,e_2,\cdots,e_n)$ 下的关系矩阵。

设 $(e_1',e_2',\cdots,e_n')$ 为 $D^{(n)}$ 的任一基，有

$$e_i' = \sum_{j=1}^{n} p_{ij} e_j$$

则 $\boldsymbol{P}=(p_{ij})\in L_n(D)$，但对子模 K 的生成集，不能有如此确切的结论。

设 $\boldsymbol{Q}=(q_{ki})\in L_m(D)$，则 $\boldsymbol{Q}^{-1}=(q_{ki}^*)\in L_m(D)$，令

$$f_k' = \sum_{l=1}^{m} q_{kl} f_l, k = 1,2,\cdots,m$$

则 $(f_1',f_2',\cdots,f_m')$ 是 K 的另一生成集，这是因为 $f_k'\in K$，且 $\forall f_r, r=1,2,\cdots,m$，有

$$\sum q_{rk}^* f_k' = \sum_k \sum_l q_{rk}^* q_{kl} f_l = f_r$$

因而 $(f_1',f_2',\cdots,f_m')$ 关于任一基的关系矩阵为

$$\boldsymbol{A}' = \boldsymbol{QAP}^{-1}$$

此处，$\boldsymbol{P}^{-1}=(p_{ij}^*)$，这只需注意下式即可得此结论

$$f_k' = \sum_l q_{kl} f_l = \sum_l \sum_j q_{kl} a_{lj} e_j = \sum_l \sum_j \sum_i q_{kl} a_{lj} p_{ji}^* e_i'$$

由此，会使我们考虑一个问题，即如何选取 $\boldsymbol{P},\boldsymbol{Q}$，使 $\boldsymbol{A}'$ 的形式最简单。为此，将引入矩阵等价的定义和矩阵的规范形等问题，读者将会看到，由此得出的一些结果和线性代数中相应的结果是平行的，但由于其表述和处理问题的手法有一些新鲜之处，我们还是不厌其烦地赘述于后。

定义 4.3.1 设 D 是主理想整环，如果 $\exists \boldsymbol{P}\in L_m(D)$，$\boldsymbol{Q}\in L_n(D)$，使 $\boldsymbol{B}=\boldsymbol{PAQ}$，则称 $\boldsymbol{A},\boldsymbol{B}$ 是等价的。

$\boldsymbol{A}$ 与 $\boldsymbol{B}$ 等价记做 $\boldsymbol{A}\sim\boldsymbol{B}$。显然 ~ 是 $M_{m,n}(D)$ 中的等价关系。

定理 4.3.2 设 $\boldsymbol{A}\in M_{m,n}(D)$，则 $\boldsymbol{A}\sim \mathrm{diag}\{d_1,\cdots,d_r,0,\cdots,0\}$，$d_i\neq 0$，$i=1,2,\cdots,r$，若 $i\leqslant j\Rightarrow d_i\mid d_j$。

首先，与线性代数相同，引入以下 3 种初等矩阵。

(1) $\boldsymbol{T}_{ij}(b)=1+be_{ij}$，$b\in D$，$i\neq j$，其中 e_{ij} 为第 i 行 j 列处是 1，且其余元素全是 0 的矩阵；

(2) $\boldsymbol{D}_i(u)=1+(u-1)e_{ii}$，$u$ 是 D 中的可逆元，显然 $\boldsymbol{D}_i(u)$ 为第 i 个对角线上元素是 u，且其余元素全是 1 的对角矩阵；

(3) $\boldsymbol{P}_{ij}=1-e_{ii}-e_{jj}+e_{ij}+e_{ji}$。

用上述 3 种初等矩阵左(右)乘 $\boldsymbol{A}$，相当于对 $\boldsymbol{A}$ 的行(列)做初等变换，这样变换得出的矩阵与 $\boldsymbol{A}$ 等价。

再对定理 4.3.2 进行证明。

证 ①设 D 是欧氏环，令 $\delta:D\to N$。

若 $\boldsymbol{A}=0$，结论显然成立。

若 $\boldsymbol{A}\neq 0$，令 a_{ij} 是 $\boldsymbol{A}$ 的所有 $\delta(a_{ij})$ 中最小的非零元素，运用初等变换将 a_{ij} 变到(1,1)位置，并设为 a_{11}。

设 $k>1$，$a_{1k}=a_{11}b_k+b_{1k}$，其中 $\delta(b_{1k})<\delta(a_{11})$，做初等变换，将第 j 列减去第 1 列的 b_k 倍，这个初等变换用 b_{1k} 代替 a_{1k}，若 $b_{1k}\neq 0$，得到等价于 $\boldsymbol{A}$ 的矩阵；若非零元的极小 δ 值比 $\boldsymbol{A}$ 的其他元素 δ 值都小，重复上述步骤并对列做相应变换，而"次" δ 是非负整数，重复有限步后，得等价矩阵

$$\begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & c_{22} & \cdots & c_{2n} \\ \vdots & & & \vdots \\ 0 & c_{m2} & \cdots & c_{mn} \end{pmatrix}$$

对 $\forall k,l$，还可令 $b_{11}\mid c_{kl}$，因若不然，$b_{11}\nmid c_{kl}$，将 k 行加到第一行，重复上面的方法，用一个 δ 值比 b_{11} 小的非零元代替 c_{kl}，经有

限步后,可得与 **A** 等价的矩阵,且 $b_{11} \mid c_{kl}(\forall k, l)$。

现对矩阵 (c_{kl}) 重复上述步骤,可得与 **A** 等价的对角阵 $\mathrm{diag}\{d_1, d_2, \cdots, d_r, 0, \cdots, 0\}$,其中,$i \leqslant j$ 时,$d_i \mid d_j$。

②设 D 是一般的主理想整环,$\forall 0 \neq a \in D$,若 $a = p_1 p_2 \cdots p_r$,p_i 是素元,定义 a 的长度 $l(a) = r$,若 u 是单位,则规定 $l(u) = 0$,对 $l(a)$ 用归纳法证明。

设

$$\mathbf{A}^* = \begin{pmatrix} x & s & & & & \\ y & t & & 0 & & \\ & & 1 & & & \\ & & & \ddots & & \\ & 0 & & & & \\ & & & & & 1 \end{pmatrix}$$

此处 $\begin{pmatrix} x & t \\ y & t \end{pmatrix}$ 是可逆阵。

同①中一样,设 $a_{11} \neq 0$,$l(a_{11}) < l(a_{ij})$,若 $a_{11} \nmid a_{1k}$,互换第 2 列与第 k 列,可设 $a_{11} \nmid a_{12}$,设 $a = a_{11}$,$b = a_{12}$,令 $d = (a, b)$,则 $l(d) < l(a)$,且 $\exists x, y \in D$,使 $ax + by = d$,令 $s = bd^{-1}$,$t = -ad^{-1}$,得

$$\begin{pmatrix} -t & s \\ y & -x \end{pmatrix} \begin{pmatrix} x & s \\ y & t \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

故 $\mathbf{A}^*$ 是可逆阵。用 $\mathbf{A}^*$ 右乘矩阵 **A** 得

$$\mathbf{A}\mathbf{A}^* = \begin{pmatrix} d & 0 & b_{13} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & & b_{2n} \\ \vdots & & & & \vdots \\ b_{m1} & b_{m2} & \cdots & & b_{mn} \end{pmatrix}$$

且 $l(d) < l(a_{11})$。

按这个步骤重复下去，并对行做同样步骤的变换，得

$$B = \begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & c_{22} & \cdots & c_{2n} \\ \vdots & & & \vdots \\ 0 & c_{m2} & \cdots & c_{mn} \end{pmatrix}$$

由于长度是非负整数，且不断减小，同欧氏环的情形一样，必到某一步为止，故得结论。

在以上定理证明中得到的对角阵是一种重要的规范形，我们称为 A 的法式。对角线上的元素称为 A 的不变因子，任一不变因子除相差单位外，是惟一的。下面用 A 的元素导出这个结论。

定理 4.3.3 令 $A \in M_{m,n}(D)$，秩 $A = r$，$\forall\, i \leqslant r$，令 Δ_i 为 A 的 i 行子式的最大公因式，则 A 的任一不变因子组与 $d_1 = \Delta_1$，$d_2 = \Delta_2\Delta_1^{-1}, \cdots, d_r = \Delta_r\Delta_{r-1}^{-1}$ 只差单位乘数。

证 首先注意到，秩 $A = r \Leftrightarrow A$ 有非零的 r 行子式，且每一个 $r+1$ 行子式全为零，而 i 行子式等于 $i-1$ 行子式与 D 中元素之积的和。

令 $Q = (q_{ki}) \in M_{m,m}(D)$，则 $QA = \left(\sum_{j=1}^{m} q_{kj}a_{ji}\right) \in M_{m\times n}(D)$ $\Rightarrow QA$ 的行是系数在 D 内的 A 的行的线性组合 $\Rightarrow QA$ 的 i 行子式是 A 的 i 行子式的线性组合 $\Rightarrow A$ 的 i 行子式的最大公因式是 QA 的 i 行子式的最大公因式的因子。

同理，令 $P = (p_{jl}) \in M_{n,n}(D)$，则 AP 的列是 A 的列的线性组合 $\Rightarrow A$ 的 i 行子式的最大公因式是 AP 的 i 行子式的最大公因式的因子。

综上所述，$A \sim B \Leftrightarrow A$ 与 B 的 i 行子式的最大公因式相同。令 $B = \mathrm{diag}\{d_1, d_2, \cdots, d_r, 0, \cdots, 0\}$ 是 A 的法式，由 $i \leqslant j \Rightarrow d_i \mid d_j$ 得 B 的 i 行子式的最大公因式是 $\Delta_i = d_1 d_2 \cdots d_i$，由此得出结论。

推论　$A, B \in M_{m,n}(D)$，则 $A \sim B$ 当且仅当 A 与 B 有相同的不变因子。

本节最后，将证明一个在模论中十分重要的主理想整环上的有限生成模的基本结构定理。

定理 4.3.4　如果 $M(\neq 0)$ 是主理想整环 D 上有限生成模，则 M 是循环模的直和，即 $M = \oplus_1^s D_{z_i}$，其阶理想满足

$$\text{ann } z_1 \supset \text{ann } z_2 \supset \cdots \supset \text{ann } z_s$$

其中 $\forall k = 1, 2, \cdots, s$，$\text{ann } z_k \neq D$。

注 1　若 $\text{ann } z_k = D \Rightarrow 1 \in D = \text{ann } z_k \Rightarrow 1 \cdot z_k = z_k = 0$，此为矛盾。

注 2　循环模的任二生成元有相同的阶理想，这是因为，若 $b \in \text{ann } z \Rightarrow b(az) = a(bz) = 0 \Rightarrow \text{ann } z \subset \text{ann } az$。反之，视 az 为生成元，有 $\text{ann } az \subset \text{ann } z \Rightarrow \text{ann } z = \text{ann } az$。故 $\text{ann } z$ 与 D_z 的生成元 z 的取法无关。

证　设 $M = \langle x_1, x_2, \cdots, x_n \rangle$，则存在满同态

$$\eta: D^{(n)} \to M$$

$$\sum a_i e_i \to \sum a_i x_i$$

使 $\eta(e_i) = x_i, i = 1, 2, \cdots, n$。其中 $D^{(n)} = \langle e_1, e_2, \cdots, e_n \rangle$，因此 $M \cong D^{(n)}/K$，$K = \ker \eta$，并设 K 由有限个元生成，即

$$K = \langle f_1, f_2, \cdots, f_m \rangle$$

而 $f_j = \sum_{i=1}^{n} a_{ji} e_i$，故 $A = (a_{ji}) \in M_{n,m}(D)$。

现用 e_i' 代替 e_i，$e_i' = \sum_{j=1}^{n} p_{ij} e_j$，$P = (p_{ij}) \in L_n(D)$，$f_k'$ 代替 f_k，$f_k' = \sum_{l=1}^{m} q_{kl} f_l$，$Q = (q_{kl}) \in L_m(D)$。

由前面的讨论知，$\{f_k'\}$ 对 $\{e_i'\}$ 的关系矩阵是 QAP^{-1}，由定理

4.3.2,可选适当的 P,Q,使

$$QAP^{-1} = \text{diag}\{d_1,d_2,\cdots,d_r,0,\cdots,0\}$$

$d_i\neq0,i=1,2,\cdots,r$,且若 $i\leqslant j\Rightarrow d_i\mid d_j\Rightarrow\{f_k'\}$和$\{e_i'\}$之间存在关系

$$f_1' = d_1e_1',\cdots,f_r' = d_re_r',f_{r+1}' = \cdots = f_m' = 0$$

现令 $y_i = \sum_{j=1}^{n}p_{ij}x_j,1\leqslant i\leqslant n$,则 $y_1,y_2,\cdots,y_n$ 是M 的另一组生成元,且 $\eta(e_i') = y_i$。

由 $d_ie_i' = f_i'\in K\Rightarrow\forall i\,(1\leqslant i\leqslant r),\ d_iy_i = d_i\eta(e_i') = \eta(d_ie_i')=\eta(f_i')=0$。而当 $r<i\leqslant n$ 时,$d_i=0$,更有 $d_iy_i=0$。

现设 $\sum_{i=1}^{n}b_iy_i = 0,b_i\in D\Rightarrow\sum_{i=1}^{n}b_ie_i'\in K\Rightarrow\sum_{i=1}^{n}b_ie_i' = \sum_{i=1}^{n}c_if_i' = \sum_{i=1}^{n}c_id_ie_i'$,而 $D^{(n)} = \langle e_1',e_2',\cdots,e_n'\rangle$,故 $b_i = c_id_i$,$1\leqslant i\leqslant n\Rightarrow b_iy_i = c_id_iy_i = 0$。故 $M=\bigoplus_1^n Dy_i$。

又由 $b_iy_i = 0$,而 $d_iy_i = 0\Rightarrow b_i\in(d_i)\Rightarrow\text{ann }y_i = (d_i)$,由 d_i 的整除性得$(d_1)\supset(d_2)\supset\cdots\supset(d_n)$。

若 d_i 是单位,由 $d_iy_i=0\Rightarrow y_i=0$,这些元素可以从生成集中去掉,故

$$M = \bigoplus_1^s Dz_i,s\leqslant n,Dz_j\neq0,j = 1,2,\cdots,s$$

其阶理想满足

$$\text{ann }z_1\supset\text{ann }z_2\supset\cdots\supset\text{ann }z_s$$

习题 4.3

1. 设 K 是由$f_1=(1,0,-1),f_2=(2,-3,1),f_3=(0,3,1),f_4=(3,1,5)$生成的 $\mathbf{Z}^{(3)}$ 的子模,求 K 的基。

2. 求由 $f_1=(2\lambda-1,\lambda,\lambda^2+3)$, $f_2=(\lambda,\lambda,\lambda^2)$, $f_3=(\lambda+1,2\lambda,2\lambda^2-3)$生成的 $\mathbf{Q}[\lambda]^{(3)}$ 的子模的基。

3. 设 $\mathbf{Z}^{(3)}$ 的 $\mathbf{Z}$-子模是由满足条件

$$x_1+2x_2+3x_3=0$$
$$x_1+4x_2+9x_3=0$$

的一切(x_1,x_2,x_3)构成的,求这个子模的基。

4. 求整数矩阵

$$\begin{pmatrix} 6 & 2 & 3 & 0 \\ 2 & 3 & -4 & 1 \\ -3 & 3 & 1 & 2 \\ -1 & 2 & -3 & 5 \end{pmatrix}$$

的法式。

5. 在 $M_4(Q[\lambda])$中,求矩阵

$$\boldsymbol{A}=\begin{pmatrix} \lambda-17 & 8 & 12 & -14 \\ -46 & \lambda+22 & 35 & -41 \\ 2 & -1 & \lambda-4 & 4 \\ -4 & 2 & 2 & \lambda-3 \end{pmatrix}$$

的法式,其中 λ 是未定元;并求可逆阵 $\boldsymbol{P},\boldsymbol{Q}$,使 $\boldsymbol{PAQ}$ 为所求的法式。

6. 利用定理 4.3.3,求

$$\begin{pmatrix} \lambda+1 & 2 & -6 \\ 1 & \lambda & -3 \\ 1 & 1 & \lambda-4 \end{pmatrix}$$

的不变因子。

7. 证明:

(i)若 D 为欧氏环,则 $M_n(D)$中的任意可逆矩阵 $\boldsymbol{A}$ 都是初等阵的乘积;

(ⅱ)定理 4.3.2 中(3)型初等阵是(1),(2)型初等阵之乘积,从而证明若 D 是欧氏环,则 $M_n(D)$ 中可逆阵都是(1),(2)型初等阵之积。

8. 若 F 是域,证明:$M_n(F)$ 中行列式为 1 的矩阵可表为(2)型初等阵之积。

9. 设 D 为主理想整环,$a_i \in D(1 \leqslant i \leqslant n)$,$d$ 是这些 a_i 的最大公约元,证明:存在 $M_n(D)$ 中的可逆矩阵 $\boldsymbol{Q}$,满足

$$(a_1, \cdots, a_n)\boldsymbol{Q} = (d, 0, \cdots, 0)$$

10. 证明:若 $a_{11}, \cdots, a_{1n}$ 在主理想整环 D 中互素,则存在 $a_{kj} \in D$,$2 \leqslant k \leqslant n, 1 \leqslant j \leqslant n$,使方阵$(a_{ij})$在 $M_n(D)$ 中可逆。

11. 设 $\boldsymbol{A} \in M_n(D)$,其中 D 为欧氏环,若 $\det \boldsymbol{A} \neq 0$,证明:存在可逆矩阵 $\boldsymbol{P} \in M_n(D)$,使得 $\boldsymbol{PA}$ 是上三角形矩阵

$$\begin{pmatrix} d_1 & b_{12} & \cdots & b_{1n} \\ 0 & d_2 & \cdots & b_{2n} \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & d_n \end{pmatrix}$$

其中对角元 $d_i \neq 0$,且 $\delta(b_{ji}) < \delta(d_i), \forall i = 1, 2, \cdots, n$。

12. 确定 $\mathbf{Z}^{(3)}/K$ 的结构,其中 K 是由 $f_1 = (2, 1, -3), f_2 = (1, -2, 2)$生成的子模。

13. 设 D 是高斯整数环 $\mathbf{Z}[\sqrt{-1}]$,试确定 $D^{(3)}/K$ 的结构,其中 K 是由 $f_1 = (1, 3, 6), f_2 = (2+3i, -3i, 12-18i), f_3 = (2-3i, 6+9i, -18i)$生成的子模,此处 $i = \sqrt{-1}$,并证明 $M = D^{(3)}/K$ 是有限的。

14. 设 M 是 $\mathbf{Z}[x]$中由 2 和 x 生成的理想,证明 M 不是循环 $\mathbf{Z}[x]$-模的直和。

15. 设 N 是 M 的子模,$x \in M$,证明:

(ⅰ) $\mathrm{ann}\,(x+N)\supseteq\mathrm{ann}\,x$；$\mathrm{ann}\,(x+N)\supsetneqq\mathrm{ann}\,x$ 当且仅当 $Dx\cap N\neq0$；

(ⅱ) $l(x+N)\leqslant l(x)$；$l(x+N)<l(x)$ 当且仅当 $Dx\cap N\neq0$（规定 $l(0)=\infty$，且当 $\mathrm{ann}\,(x)=(d)$ 时，$l(x)=l(d)$）。

16. 设 $x_1,x_2,\cdots,x_n$ 是 M 的 n 个生成元（$n\geqslant1$），并且 $y=\sum_{i=1}^{n}a_ix_i$，其中 $a_1,a_2,\cdots,a_n$ 的最大公约元为 1，即 $(a_1,\cdots,a_n)=1$，证明：存在 n 个生成元 $y_1,y_2,\cdots,y_n$ 且 $y_1=y$。

17. 设 $x_1,x_2,\cdots,x_n$ 是 M 的生成元，满足：

(ⅰ) n 最小；

(ⅱ) $l(x_1)$ 在 M 中的所有 n 个生成元中最小。

证明：$M=Dx_1\oplus N$，其中 $N=\sum_{j=2}^{n}Dx_j$，且 $\mathrm{ann}\ x_1\supsetneqq\mathrm{ann}\ y$（$\forall y\in N$）成立，由此对 n 可用归纳法证明主理想整环上有限生成模的基本结构定理。

§4.4 扭模

§4.3 中主理想整环上的有限生成模的基本结构定理给出的分解一般是不惟一的，例如，设 M 的一组基为 $\{e_i\mid1\leqslant i\leqslant n\}$，则 $M=\oplus_1^n De_i$，且 $\mathrm{ann}\ e_i=0$，又设 $\{f_i\mid1\leqslant i\leqslant n\}$ 是另一组基，且 f_i 不简单地是 e_i 在某次序下的倍数，则有第二个直和分解，显然与第一个直和分解不相同。但我们指出，任意两个这样的分解都有相同的阶理想序列。为证此结论，首先引入几个概念。

定义 4.4.1 设 M 是主理想整环 D 上的有限生成模，则称

$$\mathrm{tor}\ M\triangleq\{y\mid\exists0\neq a\in D,使\ ay=0\}$$

为 M 的扭子模。

由定义直接可得下面的命题。

命题 4.4.1 $y \in \text{tor } M \Leftrightarrow \text{ann } y \neq 0$。

命题 4.4.2 $\text{tor } M \leqslant M$。

运用子模定义可以直接验证命题 4.4.1 和命题 4.4.2 的正确性,留给读者。

运用扭子模的概念可得下面的第二结构定理。

定理 4.4.1 (第二结构定理)

任何一个主理想整环 D 上的有限生成模 M 是它的扭子模与自由子模的直和。

证 由基本结构定理 $M = \oplus_1^s Dz_i$,且

$$\text{ann } z_1 \supset \text{ann } z_2 \supset \cdots \supset \text{ann } z_s$$

若 $i \leqslant r$,有 $\text{ann } z_i \neq 0$,由命题 4.4.1 知 $z_i \in \text{tor } M$,故 $\oplus_1^r Dz_i \subset \text{tor } M$。

另一方面,$\forall\, y = \sum_{i=1}^{s} b_i z_i \in \text{tor } M$,则 $\exists\, 0 \neq a \in D$,使得 $0 = ay = \sum_{i=1}^{r} ab_i z_i = 0$,由直和性质,$\forall\, i = 1,2,\cdots,s$,有 $ab_i z_i = 0$,当 $i > r$ 时,由 $\text{ann } z_i = 0 \Rightarrow ab_i = 0$,又因 D 是整环,而 $a \neq 0 \Rightarrow b_i = 0 \Rightarrow y = \sum_{i=1}^{r} b_i z_i \in \oplus_1^r Dz_i$。故有

$$\text{tor } M = \oplus_1^r Dz_i$$

再看 $Dz_{r+1} \oplus \cdots \oplus Dz_s$,显然是 M 的子模,而 M 是主理想整环 D 上的自由模,由定理 4.3.1,其子模必为自由模,记这个子模为 K,故有

$$M = \text{tor } M \oplus K$$

下面对 $\text{tor } M$ 做进一步的研究和分解。

定义 4.4.2 设 M 为主理想整环 D 上的有限生成模,若 p 为 D 中的素元,则称

$$M_p = \{y \mid \exists\, k \in \mathbf{N}, \text{使 } p^k y = 0\}$$

为 M 的 p-准素分支。

显然，$M_p \leqslant \text{tor } M$。

命题 4.4.3 不同素元所对应的 p-准素分支是无关的。

证 设 p_1, p_2 是两个不同的素元，往证 $M_{p_1} \cap M_{p_2} = 0$。

令 $y \in M_{p_1} \cap M_{p_2} \Rightarrow y \in M_{p_1}$ 且 $y \in M_{p_2} \Rightarrow \exists k_1 \in \mathbf{N}$，使 $p_1^{k_1} y = 0$，且 $\exists k_2 \in \mathbf{N}$，使 $p_2^{k_2} y = 0 \Rightarrow p_1^{k_1} \in \text{ann } y$，且 $p_2^{k_2} \in \text{ann } y \Rightarrow 1 = (p_1^{k_1}, p_2^{k_2}) \in \text{ann } y \Rightarrow y = 1 \cdot y = 0$。

对任意 n 个不同的素元，可类似证明。

命题 4.4.4

(1)若 $M = Dx$，其中 $\text{ann } x = (d)$，且 $d = gh$，$(g, h) = 1$，则 $M = Dy \oplus Dz$，其中 $\text{ann } y = (g)$，$\text{ann } z = (h)$。

(2)若 $M = Dy + Dz$，其中 $\text{ann } y = (g)$，$\text{ann } z = (h)$，$(g, h) = 1$，则 $M = Dx$，此处 $x = gh$。

证 (1)令 $y = hx$，$z = gx$，则 $y, z \in M$；又 $(g, h) = 1 \Rightarrow \exists a, b \in D$，使得 $ah + bg = 1$，故

$$x = (ah + bg)x = a(hx) + b(gx) = ay + bz \in Dy + Dz$$

因而 $M = Dy + Dz$。

又 $\forall u \in Dy \cap Dz$，由 $gy = ghx = dx = 0$，$hz = hgx = dx = 0$，而 (g) 是主理想，$u \in Dy$，$\exists a' \in D$，使 $u = a'y \Rightarrow gu = g(a'y) = (ga')y = a'gy = 0$。

同理，$hu = 0$。故 $u = 1u = (ah + bg)u = ahu + bgu = 0$。

因而 $M = Dy \oplus Dz$，显然，$\text{ann } y = (g)$，$\text{ann } z = (h)$。

(2) 同(1)后面的证明结果 $M = Dy \oplus Dz$，若取 $x = y + z$，由 $cx = 0 \Rightarrow cy = 0 = cz \Rightarrow c$ 是 g 和 h 的倍数 $\Rightarrow [g, h] \mid c$，而 $(g, h) = 1 \Rightarrow gh \mid c$。

又因 $gh(y + z) = 0 \Rightarrow \text{ann } x = (gh)$，题设 $(g, h) = 1$，故 $\exists a, b \in D$，使 $ah + bg = 1 \Rightarrow y = (ah + bg)y = ahy = ah(y + z) = ahx \Rightarrow$

$y \in Dx$，因而 $z = x - y \in Dx$，故 $Dx = M$。

显然，由归纳法，此命题可推广到任意有限多个，即若 $M = Dx$，ann $x = (d)$，$d = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$，则

$$M = Dx_1 \oplus Dx_2 \oplus \cdots \oplus Dx_t$$

其中 ann $x_i = (p_i^{e_i})$，$i = 1,2,\cdots,t$。

由此说明，任一循环模是准素循环模的直和，准素之意为阶理想(p^e)，因而得到下面的第三结构定理。

定理 4.4.2 （第三结构定理）

任意主理想整环 D 上有限生成的扭模是准素循环模的直和。

证 首先证明，除有限个外，几乎所有的 p-准素分支全是 0，且 tor M 是这有限个 p-准素分支的直和。

设 M 为主理想整环 D 上有限生成的扭模，令

$$M = \langle x_1, x_2, \cdots, x_n \rangle$$

则

$$M = Dx_1 + Dx_2 + \cdots + Dx_n$$

$$\text{ann } x_i = (d_i), i = 1,2,\cdots,n$$

令 $p_1, p_2, \cdots, p_n$ 是所有 d_i 的不同的素因子，则 $\forall i (1 \leqslant i \leqslant n)$，$Dx_i \subset M_{p_1} + M_{p_2} + \cdots + M_{p_n} \Rightarrow M \subset M_{p_1} + \cdots + M_{p_n}$，因而，$M = M_{p_1} + \cdots + M_{p_n}$，由命题 4.4.3，不同素数所对应的 p-准素分支是无关的 $\Rightarrow M = M_{p_1} \oplus \cdots \oplus M_{p_n}$。

现设 $p \neq p_i (i = 1,2,\cdots,n)$，$p$ 也是素元，则

$$M_p = M_p \cap (M_{p_1} + \cdots + M_{p_n}) = 0$$

这说明除有限个(所有 d_i 的不同的素因子的个数)外，几乎所有的 p-准素分支全是零。

其次，我们证明，每一个 p-准素分支都是准素循环模的直和，这由基本结构定理 M 是循环模的直和，而每一循环模是准素循

环模的直和直接推出，故每个 p-准素分支是准素循环模，详细证明如下：

由基本结构定理知，$M=\oplus_1^r Dz_i$，$\operatorname{ann} z_i=(d_i)$，满足 $\operatorname{ann} z_1 \supset \operatorname{ann} z_2 \supset \cdots \supset \operatorname{ann} z_r \Rightarrow d_1 \mid d_2 \mid \cdots \mid d_r$。

设 $d_i=p_1^{e_{1i}} p_2^{e_{2i}} \cdots p_k^{e_{ki}}$，其中 $p_1, p_2, \cdots, p_k$ 是互不相同的素元，且 $e_{j1} \leqslant e_{j2} \leqslant \cdots \leqslant e_{jr}$，$1 \leqslant j \leqslant k$，则 M 是以 $(p_j^{e_{ji}})$ 为零化子的直和。

下面证明本节开始提出的问题，尽管 M 的分解不是惟一的，但却都有相同的阶理想序列，这就是不变性定理。

定理 4.4.3 设 M 是主理想整环 D 上的有限生成模，且

$$M=\oplus_1^s Dz_i=\oplus_1^t Dw_j$$

其中，$\operatorname{ann} z_1 \supset \operatorname{ann} z_2 \supset \cdots \supset \operatorname{ann} z_s$，和 $\operatorname{ann} w_1 \supset \operatorname{ann} w_2 \supset \cdots \supset \operatorname{ann} w_t$，且这些阶理想都不为零，则 $s=t$，$\operatorname{ann} z_i=\operatorname{ann} w_i$，$1 \leqslant i \leqslant s$。

证 分成三步。

(1)归结为扭模。

设 $i \leqslant r$，$\operatorname{ann} z_i \neq 0$，$i>r$ 时，$\operatorname{ann} z_i=0$；

$j \leqslant u$，$\operatorname{ann} w_j \neq 0$，$j>u$ 时，$\operatorname{ann} w_j=0$。

则 $\operatorname{tor} M=\oplus_1^r Dz_i=\oplus_1^u Dw_j$，又

$$M/\operatorname{tor} M \cong Dz_{r+1} \oplus \cdots \oplus Dz_s \cong Dw_{u+1} \oplus \cdots \oplus Dw_t$$

它们分别是秩为 $s-r$ 和 $t-u$ 的自由模，由定理 4.2.3，可换环的自由模的秩相同 $\Rightarrow s-r=t-u \Rightarrow \operatorname{ann} z_i=0$ 的个数与 $\operatorname{ann} w_j=0$ 的个数相同，故定理的证明归结为扭模。

(2)归结为准素扭模。

设 M 是扭模，$M=\oplus_1^r Dz_i=\oplus_1^u Dw_j$，将 Dz_i 和 Dw_j 分解成准素循环模的直和，固定 p，在每个分解中，把有阶理想 (p^l)，$l=1,2,\cdots$ 的循环加项组成和，如果以 (p^l) 为阶理想的循环直和项的

个数相同，则这两个分解有相同的阶理想序列，而这两个和与 p-准素分支 M_p 一致，因此定理归结为对 M_p 的证明。

(3)设 $M=M_p$，且 $M=\oplus_1^s Dz_i=\oplus_1^t Dw_j$，则 $\mathrm{ann}\ z_i=(p^{e_i})$，$\mathrm{ann}\ w_j=(p^{f_j})$，又 $\mathrm{ann}\ z_1\supset\mathrm{ann}\ z_2\supset\cdots\supset\mathrm{ann}\ z_s\Rightarrow e_1\leqslant e_2\leqslant\cdots\leqslant e_s$，$\mathrm{ann}\ w_1\supset\mathrm{ann}\ w_2\supset\cdots\supset\mathrm{ann}\ w_t\Rightarrow f_1\leqslant f_2\leqslant\cdots\leqslant f_t$；$\forall k\in\mathbf{N}$，$p^kM=\{p^kx\mid x\in M\}\leqslant M$，且

$$M\supset PM\supset p^2M\supset\cdots$$

令 $M^{(k)}=p^kM/p^{k+1}M=\{p^kx+p^{k+1}M\mid x\in M\}$，且 $p(p^kx+p^{k+1}M)=p^{k+1}M=\bar{0}\Rightarrow(p)$零化 $M(k)$。

故 $M^{(k)}$看做 $\bar{D}=D/(p)$模(请读者自行验证)，而 p 是素数$\Rightarrow\bar{D}$ 是域$\Rightarrow M^{(k)}$是域 $\bar{D}$ 上的向量空间。

下面求 $M^{(k)}$的维数。

若 $k\geqslant e_s\Rightarrow p^kM=0$，设 $k<e_s$，并设 e_{t+1}是 $e_i>k$ 中的第一个$\Rightarrow e_t\leqslant k$，而 $\mathrm{ann}\ z_t=(p^{e_t})\Rightarrow p^{e_t}z_t=0$，而 $k\geqslant e_t$，$p_kz_t=0$，又因 $M=\oplus_1^s Dz_i$，$\forall x\in M$，则 $x=d_1z_1+d_2z_2+\cdots+d_sz_s$，故 $p^kx=p^kd_{t+1}z_{t+1}+\cdots+p^kd_sz_s$，即

$$p^kM=D_{p^kz_{t+1}}+\cdots+D_{p^kz_s}=\langle p^kz_{t+1},\cdots,p^kz_s\rangle$$

故 $M^{(k)}=p^kM/p^{k+1}M=\langle p^kz_{t+1}+p^{k+1}M,\cdots,p^kz_s+p^{k+1}M\rangle$。

下面证明这个生成元组就是 $M^{(k)}$的基。

若$\overline{d_{t+1}}(p^kz_{t+1}+p^{k+1}M)+\cdots+\overline{d_s}(p^kz_s+p^{k+1}M)=0=p^{k+1}M$，因为这是直和分解，$\forall i=t+1,t+2,\cdots,s$，有$\overline{d_i}(p^kz_s+p^{k+1}M)=0=p^{k+1}M$，必有$\overline{d_i}=(p)$，若不然，$\overline{d_i}\neq(p)$，则$\overline{d_i}p^kz_s\notin p^{k+1}M$ 与$\overline{d_i}(p^kz_s+p^{k+1}M)=0$ 矛盾。

故 $M^{(k)}$的维数与大于 k 的e_i 的个数相同。同理，此维数与大于 k 的 f_j 的个数相同，而对 $\forall k\in\mathbf{N}$，大于 k 的 e_i 的个数等于大于 k 的 f_j 的个数$\Rightarrow s=t\Rightarrow e_i=f_i$，若不然，$\exists j$，$1\leqslant j\leqslant s$，$e_j\neq f_j$，则在

两个分解中直和项的个数不等，这与 $s=t$ 矛盾。故 ann $z_i=(p^{e_i})=$ ann $w_i=(p^{f_i})$。

综上所述，为今后讨论方便起见，我们给出定义。

定义 4.4.3 设 M 是主理想整环 D 上的有限生成模，则 M 有惟一的阶理想序列 ann z_1，ann z_2，…，称之为模 M 的不变因子理想，若 M 是扭模，在 M 分解成准素循环子模的直和中，这些准素循环子模的阶理想是不变的，称这些阶理想为扭模 M 的初等因子理想。

本节的最后，将结构定理应用于有限生成 Abel 群，就得到群论中的著名定理——有限生成 Abel 群的结构定理。

定理 4.4.4 任意有限生成的 Abel 群是有限 Abel 群与自由群的直和，自由部分的秩是不变的，而有限 Abel 群是素数方幂的循环群的直和，这些素数连同它的重数都是惟一确定的。

证 令主理想整环 $D=\mathbf{Z}$，则 $\mathbf{Z}$ 上的有限生成模 M 就是有限生成的 Abel 群，由基本结构定理

$$M=\langle z_1\rangle\oplus\langle z_2\rangle\oplus\cdots\oplus\langle z_s\rangle$$

其中 $\langle z_i\rangle$ 是循环群，且 ann $z_i=(d_i)$，$d_1\mid d_2\mid\cdots\mid d_s$。

将 d_i 正规化成非负的。若 $d_i>0$，则 $\circ(z_i)=|\langle z_i\rangle|=d_i$；若 $d_i=0$，则 $\circ(z_i)=\infty$。

相应于扭模的扭子群是 M 中有限阶元素生成之集，即 tor $M=\langle z_1\rangle\oplus\langle z_2\rangle\oplus\cdots\oplus\langle z_r\rangle$，此处 $d_1>0,d_2>0,\cdots,d_r>0$，但 $d_{r+1}=0$，由 $i\leqslant r$ 时 $|\langle z_i\rangle|=d_i\Rightarrow|\text{tor } M|=\prod\limits_{i=1}^{r}d_i$，故由第二结构定理得本定理的第一部分。

将第三结构定理应用于 tor M，得本定理的第二部分。

本定理指出，有限 Abel 群分解成素数方幂的循环群的直和时，素数及其重数是惟一确定的，称这些素数及其重数为有限

Abel 群的不变量。

推论 两个有限 Abel 群同构当且仅当它们有相同的不变量。

习题 4.4

1. 设 $D=\mathbf{R}[\lambda]$，M 是循环模的直和，其阶理想分别是由 $(\lambda-1)^3$，$(\lambda^2+1)^2$，$(\lambda-1)(\lambda^2+1)^4$，$(\lambda+2)(\lambda^2+1)^2$ 生成的，试确定 M 的初等因子和不变因子。
2. 证明：主理想整环 D 上的扭模 M 是既约的当且仅当 $M=Dz$，$\operatorname{ann} z=(p)$，p 是素元；并证明若 M 是有限生成的，则 M 是不可分解的（M 不能表述为两个非零子模的直和），充要条件是 $M=Dz$，其中 $\operatorname{ann} z=(p^e)$，$p$ 为素元。
3. 主理想整环 D 上有限生成模 M 的秩定义为自由模 $M/\operatorname{tor} M$ 的秩。证明：若 $M\cong D^{(n)}/K$，则秩 $M=n-$ 秩 K；并证明：若 N 为 M 的子模，则 N 和 M/N 都是有限生成的，且秩 $M=$ 秩 N $+$ 秩 M/N。
4. 设 M 是主理想整环 D 上的扭模，不变因子理想为 $(d_1)\supset(d_2)\supset\cdots\supset(d_s)$，证明：$M$ 的任意同态像 $\overline{M}$ 是扭模，且不变因子理想 $(\overline{d_1})\supset(\overline{d_2})\supset\cdots\supset(\overline{d_t})$ 满足条件 $t\leqslant s$，$\overline{d_t}\mid d_s$，$\overline{d_{t-1}}\mid d_{s-1}$，$\cdots$，$\overline{d_1}\mid d_{s-t+1}$。
5. 证明：上题中的结论把 $\overline{M}$ 改为 M 的子模 N 也是正确的。
6. 设 $\boldsymbol{A},\boldsymbol{B}\in M_n(D)$，$\det \boldsymbol{AB}\neq 0$，$D$ 是主理想整环，设 $\operatorname{diag}[a_1,a_2,\cdots,a_n]$，$\operatorname{diag}[b_1,b_2,\cdots,b_n]$，$\operatorname{diag}[c_1,c_2,\cdots,c_n]$ 分别是 $\boldsymbol{A}$，$\boldsymbol{B}$，$\boldsymbol{AB}$ 的标准型，证明：对 $1\leqslant i\leqslant n$，有 $a_i\mid c_i$，$b_i\mid c_i$。
7. 称 M 的子模 N 是纯子模，如果对任意 $y\in N$，$a\in D$，方程 $ax=y$ 在 M 中有解当且仅当在 N 中有解。证明：若 N 是直和项，则 N 是纯子模；若 N 是 M 的纯子模，且 $\operatorname{ann}(x+N)=$

(d),则可在陪集 $x+N$ 中选个代表元 x',使 $\operatorname{ann} x'=(d)$。

8. 证明:若 N 是主理想整环 D 上有限生成扭模 M 的纯子模,则 N 是 M 的直和项。
9. 设 M 是主理想整环 D 上有限生成的扭模,证明:任意循环模 Dz(其中 $\operatorname{ann} z\subset\operatorname{ann} x$ 对一切 $x\in M$ 均成立)是纯子模,从而上题中的 Dz 是直和项。

§4.5 F[λ]模

我们知道,域 F 上的多项式环 $F[\lambda]$(其中 λ 是不定元)是主理想整环,用 $F[\lambda]$ 代替 D,则 $F[\lambda]$ 上的模称为 $F[\lambda]$ 模。当把域 F 上的有限维向量空间 V 视为 $F[\lambda]$ 模时,可以导出有限维向量空间的一个线性变换理论。

定义 4.5.1 设 δ 是域 F 上的有限维向量空间 V 的线性变换,$\forall f(\lambda)=\sum_{i=0}^{m}a_i\lambda^i\in F[\lambda]$,$\forall x\in V$,定义作用乘法

$$f(\lambda)\cdot x\triangleq\sum_{i=0}^{m}a_i\sigma^i(x)$$

则 V 是一个模,称 V 为 $F[\lambda]$ 模,显然,$\sigma(x)=\lambda x$。

命题 4.5.1 $F[\lambda]$ 模 V 是扭模。

证 $\forall x\in V$,取序列 $x,\lambda x,\lambda^2x,\cdots$,因 V 在 F 上是 n 维向量空间,故 $\exists\, m\leqslant n$,使

$$\lambda^m x=a_0x+a_1\lambda x+\cdots+a_{m-1}(\lambda^{m-1}x)$$
$$a_i\in F,0\leqslant i\leqslant m-1$$

则有

$$f(\lambda)=\lambda^m-a_{m-1}\lambda^{m-1}-\cdots-a_0\neq 0$$

但

$$f(\lambda)\cdot x=0\Rightarrow f(\lambda)\in\operatorname{ann} x\Rightarrow x\in\operatorname{tor} V$$

故 V 是扭模。

设 V 在 F 上的基是 $u_1, u_2, \cdots, u_n$，一般说来，$\{u_i \mid 1 \leqslant i \leqslant n\}$ 不一定是 $F[\lambda]$ 模 V 的基，设 $F[\lambda]^{(n)}$ 的基为 $(e_1, e_2, \cdots, e_n)$，则存在同态 $\eta: F[\lambda]^{(n)} \to V$，使 $\eta(e_i) = u_i$，$i = 1, 2, \cdots, n$，并有 $F[\lambda]^{(n)}/K \cong V$，其中 $K = \ker \eta$。

下面的命题给出求 K 的基的方法。

命题 4.5.2 设 σ 是 V 的线性变换，$\sigma(u_i) = \sum\limits_{j=1}^{n} a_{ij} u_j$，$i = 1, 2, \cdots, n$，则 K 的基由 $f_i = \lambda e_i - \sum\limits_{j=1}^{n} a_{ij} e_j$，$1 \leqslant i \leqslant n$ 所组成。

证 因 $\eta(f_i) = \lambda \eta(e_i) - \sum\limits_{j=1}^{n} a_{ij} \eta(e_j) = \lambda u_i - \sigma(u_i) = 0$，故 $f_i \in \ker \eta = K$，$i = 1, 2, \cdots, n$。

由 $\lambda e_i = f_i + \sum\limits_{j=1}^{n} a_{ij} e_j \Rightarrow \forall \sum g_i(\lambda) e_i \in F[\lambda]^{(n)}$，有 $\sum g_i(\lambda) e_i = \sum h_i(\lambda) f_i + \sum b_i e_i$，其中，$g_i(\lambda), h_i(\lambda) \in F[\lambda]$，$b_i \in F$。

若 $\sum g_i(\lambda) e_i \in K$，而 $\sum h_i(\lambda) f_i \in K \Rightarrow \sum b_i e_i \in K \Rightarrow \sum b_i u_i = 0$，而 u_i 是 V 的基 $\Rightarrow b_i = 0$，$\forall i = 1, 2, \cdots, n$。

故 K 中元素具有形式 $\sum h_i(\lambda) f_i \Rightarrow f_i$ 是 K 的生成元。

下面证明 f_i 是 K 的基。

若有 $\sum\limits_i h_i(\lambda) f_i = 0 \Rightarrow \sum\limits_i h_i(\lambda) \cdot \lambda e_i - \sum\limits_i \sum\limits_j h_i(\lambda) a_{ij} e_j = 0$，而 e_i 是 $F[\lambda]^{(n)}$ 的基 $\Rightarrow h_i(\lambda) \cdot \lambda = \sum\limits_j h_j(\lambda) \cdot a_{ji}$。

今断言，$\forall i$，$h_i(\lambda) = 0$，若不然，$\exists h_i(\lambda) \neq 0$，令 $h_r(\lambda)$ 是不等于 0 的次数最大的一个，显然有

$$h_r(\lambda)\cdot\lambda \neq \sum h_j(\lambda)\cdot a_{ji}$$

此为矛盾，故 f_i 是 K 的基。

K 的基 (f_i) 对 $F[\lambda]^{(n)}$ 的基 (e_i) 的关系矩阵为 $\lambda\boldsymbol{I}-\boldsymbol{A}$，$\lambda\boldsymbol{I}-\boldsymbol{A}$ 的法式给出 V 的不变因子，从而给出循环子模的直和分解。

定义 4.5.2 令 $\boldsymbol{A}\in M_n(F)$，F 是域，设 $f(\lambda)=\det(\lambda\boldsymbol{I}-\boldsymbol{A})$，称 $f(\lambda)$ 是 $\boldsymbol{A}$ 的特征多项式。

设 $f(\lambda)=\lambda^n-a_1\lambda^{n-1}+\cdots+(-1)^n a_n$，称 $a_1=\sum\limits_{i=1}^{n}a_{ii}$ 为 $\boldsymbol{A}$ 的迹，记做 $\operatorname{tr}\boldsymbol{A}$，$a_n=\det\boldsymbol{A}$，$a_i$ 是 $\boldsymbol{A}$ 的 i 行主子式的和，$f(\lambda)$ 是 $\lambda\boldsymbol{I}-\boldsymbol{A}$ 的不变因子的乘积，由于 V 是扭模，这些不变因子都不为 0，故 $\lambda\boldsymbol{I}-\boldsymbol{A}$ 的法式为

$$\operatorname{diag}\{1,\cdots,1,d_1(\lambda),\cdots,d_s(\lambda)\}$$

此处，$d_i(\lambda)$ 是首项系数为 1 的正次数的多项式，且 $i\leqslant j$ 时，$d_i(\lambda)\mid d_j(\lambda)$。故 $\exists\,\boldsymbol{P},\boldsymbol{Q}\in L_n(F[\lambda])$，使得

$$\boldsymbol{P}(\lambda\boldsymbol{I}-\boldsymbol{A})\boldsymbol{Q}=\operatorname{diag}\{1,\cdots,1,d_1(\lambda),\cdots,d_s(\lambda)\}$$

记 $\boldsymbol{Q}^{-1}=(q_{ij}^*)$，而令 $v_i=\sum q_{ij}^*u_j$，u_j 是 $F[\lambda]$ 模 V 的生成元，$Z_i=v_{n-s+i}$，则有

$$V=F[\lambda]_{z_1}\oplus F[\lambda]_{z_2}\oplus\cdots\oplus F[\lambda]_{z_s}$$

此处，$\operatorname{ann} z_i=(d_i(\lambda))$。

下面讨论线性变换 σ 的两种规范形。

(1)有理标准形

设 $s=1$，$V=F[\lambda]_z$ 是循环 $F[\lambda]$-模，则 $\operatorname{ann} z=(f(\lambda))$，$f(\lambda)=\det(\lambda\boldsymbol{I}-\boldsymbol{A})$，而 $f(\lambda)$ 是使 $f(\lambda)z=0$ 的次数最低的多项式，故 $z_1,\lambda z_1,\cdots,\lambda^{n-1}z$ 线性无关，因而构成 V 的基，因此 σ 在此基下的关系矩阵为

$$\begin{pmatrix} 0 & 1 & 0 & & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & & & \vdots \\ 0 & & \cdots & & 0 & 1 \\ (-1)^{n-1}a_n & \cdots & & & -a_2 & a_1 \end{pmatrix}$$

称为 $f(\lambda)$的相伴矩阵。

现设 $V = F[\lambda]_{z_1} \oplus F[\lambda]_{z_2} \oplus \cdots \oplus F[\lambda]_{z_s}$，将每个 $F[\lambda]_{z_i}$ 的基排在一起，若 $\deg d_i(\lambda) = n_i$，则 σ 在基

$$(z_1, \cdots, \lambda^{n_1-1} z_1, z_2, \cdots, \lambda^{n_2-1} z_2, \cdots, z_s, \cdots, \lambda^{n_s-1} z_s)$$

下的矩阵是

$$B = \begin{pmatrix} B_1 & & & \\ & B_2 & & 0 \\ & & \ddots & \\ & 0 & & \\ & & & B_s \end{pmatrix}$$

此处 B_i 是 $d_i(\lambda)$的相伴矩阵，称 B 为 σ 的有理标准形。

显然，一旦知道 $\lambda I - A$ 的不变因子，就可写出有理标准形，而这些不变因子可用初等变换计算出来。

(2)Jordan 标准形

如果不变因子可分解成 $F[\lambda]$中一次因式 $\lambda - r$ 的乘积，此时，V 的初等因子具有形式$(\lambda - r)^e$，$r \in F$，对应每一个初等因子有一直和项 $F[\lambda]_w$，此处 $\mathrm{ann}\ w = ((\lambda - r)^e)$，故域 F 上的向量空间 $F[\lambda]_w$ 有基

$$w, (\lambda - r)w, (\lambda - r)^2 w, \cdots, (\lambda - r)^{e-1} w$$

σ 在此基下的矩阵是

$$\begin{pmatrix} r & 1 & & & \\ & r & 1 & & 0 \\ & & \ddots & \ddots & \\ & 0 & & r & 1 \\ & & & & r \end{pmatrix}$$

若 $V = F[\lambda]_{w_1} \oplus F[\lambda]_{w_2} \oplus \cdots \oplus F[\lambda]_{w_t}$，且 ann $w_i = ((\lambda - r_i)^{e_i})$，将每个 $F[\lambda]_{w_i}$ 上的基排在一起，从而得到 V 在 $F[\lambda]$ 上的基，σ 在这组基下的矩阵为

$$C = \begin{pmatrix} C_1 & & & \\ & C_2 & & 0 \\ & & \ddots & \\ & 0 & & \\ & & & C_t \end{pmatrix}$$

其中

$$C_i = \begin{pmatrix} r_i & 1 & & & \\ & r_i & 1 & 0 & \\ & & \ddots & \ddots & \\ & 0 & & r_i & 1 \\ & & & & r_i \end{pmatrix}$$

称 C 为 σ 的 Jordan 标准形。

由模论还可导出矩阵的特征多项式和最小多项式的若干典型结论，这就是下面的定理。

定理 4.5.1 令 $A \in M_n(F)$，F 是域，设 $f(\lambda) = \det(\lambda I - A)$ 是 A 的特征多项式，则 $f(A) = 0$；令 $\Delta_{n-1}(\lambda)$ 是 $\lambda I - A$ 的 $n-1$ 阶子式的首项系数为 1 的最高公因式，$m(\lambda) = f(\lambda)/\Delta_{n-1}(\lambda)$ 是

A 的最小多项式,则 $m(A)=0$,且 $m(\lambda)$是所有使 $g(A)=0$ 的 $g(\lambda)$的因子,并且 $m(\lambda)$与 $f(\lambda)$在 $F[\lambda]$中有相同的素因子。

证 $f(\lambda)=\det(\lambda I-A)$,设

$$V = F[\lambda]_{z_1} \oplus F[\lambda]_{z_2} \oplus \cdots \oplus F[\lambda]_{z_t}$$

$\operatorname{ann} z_i=(d_i(\lambda))$,当 $i\leqslant j$ 时,$d_i(\lambda)\mid d_j(\lambda)$,令 $m(\lambda)=d_t(\lambda)$,则

$$d_i(\lambda)\mid m(\lambda)\Rightarrow m(\lambda)z_i=0$$

$\forall x\in V\Rightarrow x=\sum g_i(\lambda)z_i\Rightarrow m(\lambda)x=0$,设 $m(\lambda)=\sum_{i=0}^{m} b_i\lambda^i$,$m(\lambda)x=\sum_{i=0}^{m} b_i\sigma^i(x)=m(\sigma)(x)=0\Rightarrow m(\sigma)=0$,故等价地有 $m(A)=0$。

若有 $g(\lambda)\in F[\lambda]$,$g(A)=0\Rightarrow g(\sigma)=0\Rightarrow g(\lambda)z_t=0\Rightarrow g(\lambda)\in\operatorname{ann}(m(\lambda))\Rightarrow m(\lambda)\mid g(\lambda)$,故 $m(\lambda)$是所有使 $g(A)=0$ 的 $g(\lambda)$的因子,显然 $f(A)=0$,$m(\lambda)=d_t(\lambda)=f(\lambda)/\Delta_{n-1}(\lambda)$。

又因 $d_i(\lambda)\mid m(\lambda)\Rightarrow f(\lambda)$与 $m(\lambda)$有相同的不可约因子,最多只是这些因子的重数不同。

习题 4.5

1. 确定阶数为 360 的不同构的 Abel 群的个数。
2. 验证矩阵

$$A=\begin{pmatrix}1&0&0&0\\0&1&0&0\\-2&-2&0&1\\-2&0&-1&2\end{pmatrix}$$

的特征多项式是 $Q[x]$中线性因子之积;在 $M_4(Q)$中,确定 A 的有理标准形和 Jordan 标准形,并求使 A 相似于各标准形的矩阵。

3. 证明：由线性变换 T 确定的 $F[\lambda]$-模是循环的当且仅当特征多项式 $f(\lambda)$ 就是 T 的最小多项式。

4. 证明：$M_n(F)$ 中任意幂零矩阵相似于下面形式的矩阵

$$\begin{pmatrix} N_1 & & 0 \\ & \ddots & \\ 0 & & N_s \end{pmatrix}$$

其中 N_i 具有形式

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \vdots \\ \vdots & & & \ddots & \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & & 0 \end{pmatrix}$$

5. 证明：矩阵 $\boldsymbol{A} \in M_n(\mathbf{C})$ 相似于 $\mathrm{diag}\{r_1, r_2, \cdots, r_n\}$ $(r_i \in \mathbf{C})$ 的充分必要条件是最小多项式 $m(\lambda)$ 有不同的根。

6. 证明：若 $\boldsymbol{A}^2 = \boldsymbol{A}$，则 $\boldsymbol{A} \sim \mathrm{diag}\{1, \cdots, 1, 0, \cdots, 0\}$。

7. 证明：$\boldsymbol{A}, \boldsymbol{B} \in M_n(\mathbf{C})$ 是相似矩阵当且仅当对任意的 $a \in C$，$k = 1, 2, \cdots$，秩$(a\boldsymbol{I} - \boldsymbol{A})^k$ = 秩$(a\boldsymbol{I} - \boldsymbol{B})^k$。

第5章　范　畴

在系统科学中，常常要给出系统的统一表现，即不但要研究系统本身，还要研究此系统和彼系统之间的关系，我们关心的是要把它们看做一个统一的整体来研究，这就需要范畴作为工具。

范畴是同调代数中的一个基本概念，它是1945年由Eilenberg和Maclane首先引入的。设V是域F上的一个有限维向量空间，V^*是V上的线性函数所构成的向量空间，而V^{**}又是V^*上的线性函数所构成的向量空间，称它为V的双对偶空间，Eilenberg和Maclane同时考虑所有的有限维向量空间及V和V^{**}中的线性变换，这就导致范畴、函子以及自然变换等概念的产生。

范畴作为一种工具已经应用到数学的许多领域，特别是近代数学的许多新分支都使用范畴语言来描述。例如代数几何、代数数论、系统科学以及模糊数学等，作为代数的基础课程——基础代数（或近世代数、抽象代数）等也出现了用范畴论来通观的趋势①，本书虽没有使用这样的语言去描述，但如上所述，用范畴论去通观，站在高处俯瞰全书，将受益匪浅。

本章主要介绍范畴论的一些基本概念，如函子、自然变换、积、上积、hom函子和可表函子等，所有这些，将用大量的例子来说明，使“范畴”这一比较抽象的概念变得较为具体和容易理解。

---

① 霍根佛 T W.代数学.冯克勤译.长沙:湖南教育出版社,1985

§5.1 范畴的定义

定义 5.1.1 一个范畴 $\mathscr{C}$ 由下列 3 个部分构成。

(1) 一个对象类 ob $\mathscr{C}$,类中的成员用 $A,B,C,\cdots$ 表示。

(2) 对于每对对象 (A,B),对应着一个集合 $\hom_{\mathscr{C}}(A,B)$,其中的元素 f 叫态射(morphism),记为 $f:A\to B$,称 A 为定义域,B 为上域(当 $\mathscr{C}$ 显然时,可记为 $\hom_{\mathscr{C}}(A,B)=\hom(A,B)$)。

(3) 对任意的对象组 (A,B,C),存在映射

$$\eta:\hom(A,B)\times\hom(B,C)\to\hom(A,C)$$
$$(f,g)\to gf$$

且满足下列 3 个条件:

① 若 $(A,B)\neq(C,D)$,则 $\hom(A,B)\cap\hom(C,D)=\varnothing$;

② 结合性,若 $f\in\hom(A,B)$,$g\in\hom(B,C)$,$h\in\hom(C,D)$,则 $(hg)f=h(gf)$,为此我们把任意 3 个元素相乘简记为 hgf;

③ 单位元的存在性,$\forall A\in$ ob $\mathscr{C}$,$\exists 1_A\in\hom(A,A)$,使得 $f\cdot 1_A=f$,$1_A\cdot g=g$,对 $\forall f\in\hom(A,B)$,$g\in\hom(B,A)$ 均成立。

由此可见,范畴的概念由对象的类和态射的类这两部分构成,但要特别注意,对象不一定是集合,态射又不一定是映射,但它们又分别以集合和映射的概念为特例,显然,范畴是一个相当广泛的概念。

还要注意,若 $f\in\hom(A,B)$,则和映射的记号一样,可写为 $f:A\to B$ 或 $A\xrightarrow{f}B$,我们再次强调,f 不一定是映射,仅仅是记号而已,我们还指出,gf 有定义当且仅当 g 的定义域与 f 的上域相同并且 gf 与 f 有相同的定义域,并与 g 有相同的上域。

最后必须指出，在定义 5.1.1 中，结合性可推广到任意有限多个元素，且单位元 1_A 是惟一的。

同映射一样，态射 $gf = h$ 可用图 5-1 三角形可换来表示；一般地，$gf = kh$ 可用图 5-2 矩形可换来表示。

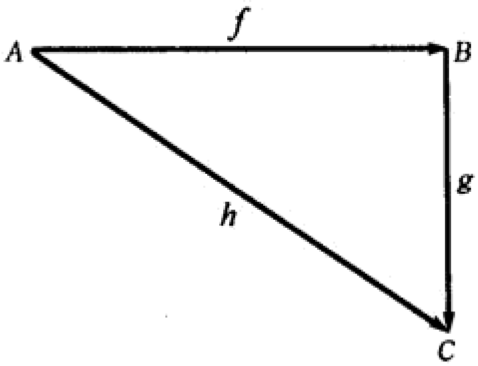


图 5-1

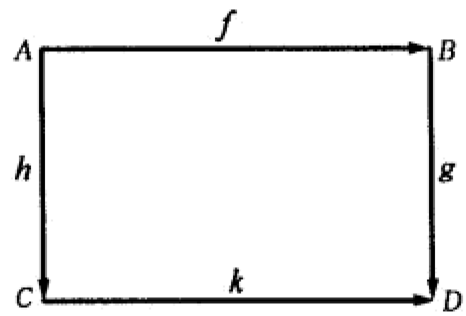


图 5-2

结合律 $(hg)f = h(gf)$ 可表示为图 5-3，对单位元 $1_A \in \hom(A,A)$，$1_A \cdot g = g$，　$f \cdot 1_A = f$ 可表示为图 5-4。

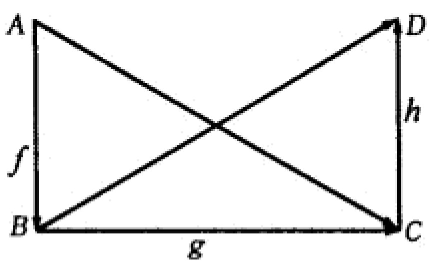


图 5-3

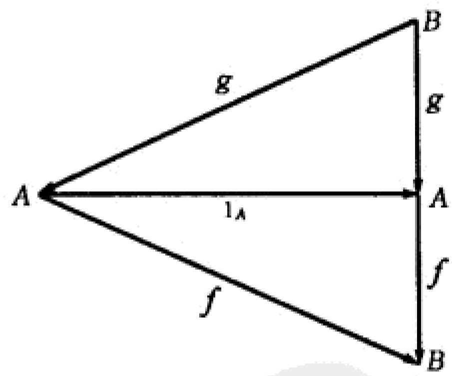


图 5-4

在定义 5.1.1 中，条件 ① 也可去掉，因可用三元序对 (A,B,f) 去代替 $\hom(A,B)$。我们强调所有的对象成一个类，所有的态射也成一个类，而不说它们成一个集合，这说明，我们只需要一个标准，用以决定一个 A 是否为范畴 $\mathscr{C}$ 的对象，而不必考察集合的公理。如果全体对象构成一个集合，全体态射也构成一个集合，此时的范畴就称为小范畴。

举几个常见的例子。

例1 集范畴**Set**,ob **Set** = 所有的集合构成的类,但对本性类

$$M = \{x \mid x \text{是一个集合,且} x \notin x\}$$

易证 M 不是集合,即 $M \notin$ ob **Set**, $\forall A,B \in$ ob **Set**,定义

$$\hom(A,B) = B^A = \{f \mid f \text{是从} A \text{到} B \text{的映射}\}$$

gf 为通常的映射的合成,1_A 为集合 A 的恒等映射,定义 5.1.1 中的 3 个条件成立是显然的。

例2 亚群范畴 **Mon**, ob **Mon** 为所有的亚群构成的类,$\hom(M,N) = \{f \mid f$ 是由亚群 M 到亚群 N 的同态映射$\}$,gf 为通常的映射合成,1_M 为恒等同态,易证这是一个范畴。

例3 群范畴 **Grp**,其定义同例 2,此处只需用群代替亚群。

例4 Abel 群范畴 **Ab**,ob **Ab** 是所有的 Abel 群构成的类,其他同例 2。

与任何一个代数结构一样,我们来定义范畴的子结构。

定义 5.1.2 范畴 $\mathscr{D}$ 称为范畴 $\mathscr{C}$ 的子范畴,如果 ob $\mathscr{D}$ 是 ob $\mathscr{C}$ 的一个子类,且 $\forall A,B \in$ ob $\mathscr{D}$,有 $\hom_{\mathscr{D}}(A,B) \subset \hom_{\mathscr{C}}(A,B)$,并且对 $A \in$ ob $\mathscr{D}$ 的单位元 1_A 和 $\mathscr{D}$ 中的态射的乘积要求与 $\mathscr{C}$ 中的相同,则子范畴表示为 $\mathscr{D} \subset \mathscr{C}$。

如果对 $\forall A,B \in$ ob $\mathscr{D}$,有 $\hom_{\mathscr{D}}(A,B) = \hom_{\mathscr{C}}(A,B)$,则称 $\mathscr{D}$ 是完满的(full)。

显然,在上面的例子中,**Ab** 是 **Grp** 的子范畴,**Grp** 是 **Mon** 的子范畴,并且它们都是完满的,而 **Mon** 却不是 **Set** 的子范畴。

令 M 是一个亚群,特别地,我们还可定义对象只有一个元素的范畴 **M**,ob **M** = $\{A\}$,并定义 $\hom(A,A) = M$,1_A 是 M 中的单位元,$\forall x,y \in \hom(A,A)$,$xy$ 就是 M 中给定的乘积,显然 ob **M** 是一个集合,故 **M** 是小范畴。

定义 5.1.3 称 $f \in \hom(A,B)$ 为同构,如果 $\exists\, g \in \hom(B,$

A)，使得 $fg = 1_B$ 且 $gf = 1_A$。

显然，g 由 f 惟一确定，可记为 f^{-1}。f^{-1} 也是同构，并可记为 $(f^{-1})^{-1} = f$。如果 f 和 h 都是同构，则 fh 也是同构，且 $(fh)^{-1} = h^{-1}f^{-1}$。在 **Set** 中，同构是双射，而在 **Grp** 中，同构就是通常的群同构。

例 5　令 G 是一个群，定义群范畴 **G**，ob **G** $= \{G\}$，hom $= (G,G) = G$，$\forall x \in \hom(G,G)$，$\exists y \in \hom(G,G)$，使 $xy = 1$，其中 1 是群 G 的单位元，故每一个态射都是同构。由此，我们可由范畴给出群的定义。

定义 5.1.4　只有一个对象的范畴，如果每个态射都是同构，那么这个范畴称为群。

定义 5.1.5　一个范畴 $\mathscr{D}$ 称为离散范畴，如果在 $\mathscr{D}$ 中定义

$$\hom(A,B) = \begin{cases} \varnothing, & \text{当 } A \neq B \text{ 时} \\ \{1_A\}, & \text{当 } A = B \text{ 时} \end{cases}$$

小离散范畴可视为对象的集合。

例 6　环范畴 **Ring**，ob **Ring** = {所有有单位元的结合环}，态射为通常的环同态映射，而无单位元的环范畴 **Rng**，其对象为所有无单位元的结合环，显然 **Ring** 是 **Rng** 的子范畴，但却不是完满的，这是因为

$$\text{ob } \mathbf{Ring} \subset \text{ob } \mathbf{Rng}$$

$$\hom_{\mathbf{Ring}}(A,B) \subset \hom_{\mathbf{Rng}}(A,B)$$

但 $\hom_{\mathbf{Ring}}(A,B) \neq \hom_{\mathbf{Rng}}(A,B)$。

例如：

$$A = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a,b \in \boldsymbol{Q} \right\}, \boldsymbol{E} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$B = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a \in \boldsymbol{Q} \right\}, \boldsymbol{E}' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

令

$$f:\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \to \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

显然，$f \in \hom_{\mathbf{Rng}}(A, B)$，但 $f \notin \hom_{\mathbf{Ring}}(A, B)$，因为

$$f\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

例 7 环 R 上的左模范畴 **R-Mod**，其中 ob **R-Mod** 是环 R 上的左模类，态射是 R- 模同态，态射的积是映射的合成，特别当 R 等于域 F 时，**R-Mod** 就是域 F 上的向量空间范畴。类似地，可定义环 R 上的右模范畴 **Mod-R**。

例 8 令 $(S, \leqslant)$ 是一个先序集，即"$\leqslant$"满足自反性和传递性，定义范畴 **S** 如下：

(1) ob $\mathbf{S} = S$；

(2) $\forall a, b \in S$，

$$\hom(a, b) = \begin{cases} \{f \mid f \in S\}, & \text{当 } a \leqslant b \text{ 时} \\ \varnothing, & \text{当 } a \nleqslant b \text{ 时} \end{cases}$$

若 $f \in \hom(a, b)$，$g \in \hom(b, c)$，则 $gf \in \hom(a, c)$，即 gf 或为单元集，或为空集。

显然，如此定义的范畴 **S** 满足范畴的定义。反之，对任何一个小范畴 **S**，若 $\forall A, B \in$ ob **S**，$\hom(A, B)$ 或是空集或是单元集，则它就是先序集 $(S, \leqslant)$ 的范畴。

例 9 拓扑空间的范畴 **Top**，ob **Top** = {所有的拓扑空间}，态射为连续映射，易证 **Top** 是一个范畴。

本节最后，将给出一个由已知范畴构造新范畴的定义。

定义 5.1.6 设 $\mathscr{C}$ 和 $\mathscr{D}$ 都是范畴，称 $\mathscr{C} \times \mathscr{D}$ 是积范畴，如果

(1) ob $\mathscr{C} \times \mathscr{D} =$ ob $\mathscr{C} \times$ ob $\mathscr{D}$；

(2) 若 $A, B \in$ ob $\mathscr{C}$，$A', B' \in$ ob $\mathscr{D}$，则

$$\hom_{\mathscr{C}\times\mathscr{D}}((A, A'), (B, B')) \triangleq \hom_{\mathscr{C}}(A, B) \times \hom_{\mathscr{D}}(A', B')$$

$$1_{(A, A')} = (1_A, 1_{A'})$$

且若 $f \in \hom_{\mathscr{C}}(A,B)$，$g \in \hom_{\mathscr{C}}(B,C)$，$f' \in \hom_{\mathscr{D}}(A',B')$，$g' \in \hom_{\mathscr{D}}(B',C')$，则

$$(g,g')(f,f') = (gf,g'f')$$

定义的合理性极易验证。

习题 5.1

1. 已知 ob **Ring*** 是所有的环构成的类，如果 R,S 是环，定义 $\hom_{\mathbf{Ring}^*}(R,S)$ 是 R 到 S 的同态映射和反同态映射的集合，态射 gf 是映射 g 和 f 的合成，1_R 是 R 的恒等映射，证明：在这些已知条件下，定义了一个 **Ring*** 范畴。
2. 所谓具有旋转的环是一个序对 (R,j)，其中 R 是一个有单位元的环，j 是 R 的旋转，也就是说，如果 $j:a \to a^*$，则 $(a+b)^* = a^* + b^*$，$(ab)^* = b^* a^*$，$1^* = 1$，$(a^*)^* = a$。所谓一个具有旋转 (R,j) 的环到具有旋转 (S,k) 的环的同态是指一个 R 到 S 的映射 η，使 η 是一个 R 到 S 的同态，且有 $\eta(ja) = k(\eta a)(\forall a \in R)$。若 ob **RinV** 是具有旋转的环构成的类，如果 (R,j)，(S,k) 是具有旋转的环，定义 $\hom((R,j),(S,k))$ 是 (R,j) 到 (S,k) 同态的集合，态射 gf 是映射的合成，$1_{(R,j)} = 1_R$，证明：在这些已知条件下，定义了一个 **RinV** 范畴。
3. 设 $\mathscr{C}$ 是一个范畴，A 是 $\mathscr{C}$ 的对象，令 ob $\mathscr{C}/A = \bigcup_{X \in \text{ob}\,\mathscr{C}} \hom(X,A)$，所以 ob $\mathscr{C}/A$ 是在 $\mathscr{C}$ 中箭头到 A 的态射类，如果 $f \in \hom(B,A)$，$g \in \hom(C,A)$，定义 $\hom(f,g)$ 是 u 的集合，其中 $u:B \to C$ 使图 5-5 可交换。对 $(f,g) \neq (f',g')$，$\hom(f,g)$ 和 $\hom(f',g')$ 相交，对于 $h:D \to A$，如果 $u \in \hom(f,g)$，$v \in \hom(g,h)$，则 $vu \in \hom(f,h)$，用这些条件来定义从 $\hom(f,g)$ 和 $\hom(g,h)$ 到 $\hom(f,h)$ 的乘积，定义 $1_f = 1_B$，其中 $f:B$

$\to A$。证明：这些已知条件能被用来定义一个范畴 $\mathscr{C}/A$，称为 $\mathscr{C}$ 在 A 上的范畴。

4. 设 $\mathscr{C}$ 是一个范畴，$A_1, A_2 \in \mathrm{ob}\,\mathscr{C}$，证明：由下面的条件定义了一个范畴 $\mathscr{C}/\{A_1, A_2\}$，其中对象是 (B, f_1, f_2)，$f_i \in \hom_{\mathscr{C}}(B, A_i)$，态射 $h:(B, f_1, f_2) \to (C, g_1, g_2)$ 是指 $\mathscr{C}$ 中的态射 $h: B \to C$，使图 5-6 可换。与范畴 $\mathscr{C}$ 一样，态射集不相交，并定义 $1_{(B, f_1, f_2)} = 1_B$，态射的合成也与 $\mathscr{C}$ 中一样定义，验证：定义 5.1.1 的条件 ② 和 ③ 成立。

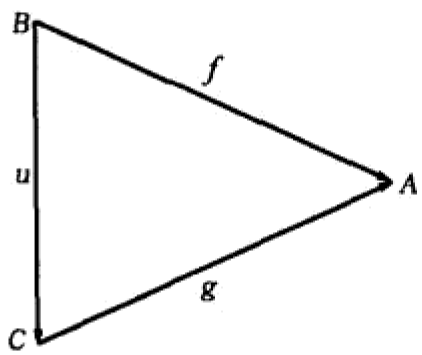


图 5-5

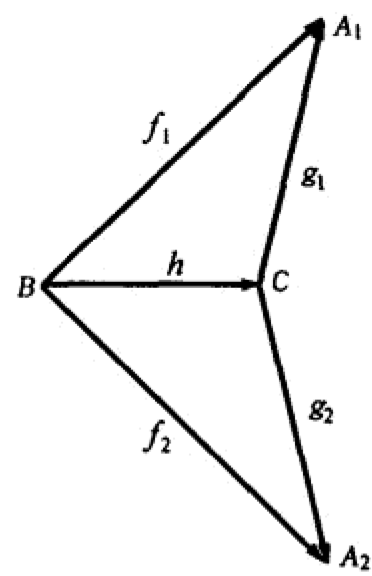


图 5-6

5. 设 **G** 是一个广群范畴，并设 $G = \bigcup_{A, B \in \mathrm{ob}\,\mathbf{G}} \hom(A, B)$，对 $\forall f, g \in G$，在 G 中定义了合成运算 fg，且满足：

(ⅰ) 对 $\forall f \in G$，存在惟一确定的元 $u, v \in G$，$uf = f = fv$，u, v 分别被称为 f 的左、右单位元；

(ⅱ) 如果 u 是单位元，则 u 是它自己的左单位元，因而也是它自己的右单位元；

(ⅲ) 乘积 fg 有定义当且仅当 f 的右单位元同 g 的左单位元一致；

(iv) 如果 fg 和 gh 有定义，则 $(fg)h, f(gh)$ 也有定义，且 $(fg)h = f(gh)$；

(v) 如果 f 有左单位元 u 和右单位元 v，则存在元素 g，它有右单位元 u 和左单位元 v，且满足 $fg = u$ 和 $gf = v$。

如果 G 是一个满足条件(i)~(v)的集合，证明 G 定义了一个广群范畴 **G**，其中 ob **G** 是 G 的单位元集合，对 $\forall u, v \in$ ob **G**，hom(u, v) 是 G 中有 u 作为左单位元和 v 作为右单位元的元素的集合，hom$(u, v) \times$ hom(v, w) 的乘积运算在 G 中给定。

6. 设 $\mathscr{C}$ 是一个小范畴，$C = \bigcup_{A, B \in \mathrm{ob}\,\mathscr{C}} \mathrm{hom}(A, B)$，证明：$\mathscr{C}$ 具有一个满足上面 5 题中条件(i)~(iv)的合成运算。反之，如果 $\mathscr{C}$ 是具有满足它们条件的合成运算，则 $\mathscr{C}$ 定义了与第 5 题一样的小范畴，试证之。

7. 设 $\mathscr{C}$ 是与第 6 题一样的范畴，设 $\mathscr{C}^*$ 是 $\mathscr{C}$ 和 $\{0\}$ 不相交的并，并通过下列规则将 $\mathscr{C}$ 中的合成推广到 $\mathscr{C}^*$ 中：

(i) $0\alpha = 0 = \alpha 0 (\forall \alpha \in \mathscr{C}^*)$；

(ii) 如果 $f, g \in \mathscr{C}$，fg 在 $\mathscr{C}$ 中没有定义，则 $fg = 0$。

证明：$\mathscr{C}^*$ 是一个半群。

§5.2 对偶原则

首先，由已知范畴 $\mathscr{C}$ 去构造一个新的范畴。

定义 5.2.1 令 $\mathscr{C}$ 是一个范畴，称 $\mathscr{C}^{OP}$ 为 $\mathscr{C}$ 的对偶范畴，如果：

(1) ob $\mathscr{C}^{OP}$ = ob $\mathscr{C}$；

(2) $\forall A, B \in$ ob $\mathscr{C}^{OP}$，则 $\mathrm{hom}_{\mathscr{C}}{}^{OP}(A, B) \triangleq \mathrm{hom}_{\mathscr{C}}(B, A)$，且若 $f \in \mathrm{hom}_{\mathscr{C}}{}^{OP}(A, B)$，$g \in \mathrm{hom}_{\mathscr{C}}{}^{OP}(B, C)$，则在 $\mathscr{C}^{OP}$ 中 g 与 f 的乘积记做 $g \circ f$，且 $g \circ f \triangleq fg$，1_A 与 $\mathscr{C}$ 中的 1_A 相同。

定义的合理性容易验证，且显然有 $(\mathscr{C}^{OP})^{OP} = \mathscr{C}$。对 $\mathscr{C}$ 的任一

交换图,若把所有的箭头方向都倒转,则得到一个有关 $\mathscr{C}^{OP}$ 的交换图。例如,在 $\mathscr{C}$ 中,若 $f: A \to B$,则在 $\mathscr{C}^{OP}$ 中有 $f: B \to A$,因而由 $\mathscr{C}$ 的三角形(图 5-7) 可换,在 $\mathscr{C}^{OP}$ 中,有图 5-8 可换。

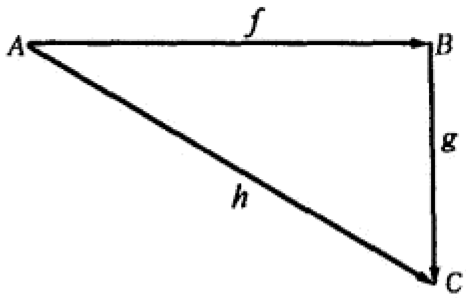


图 5-7

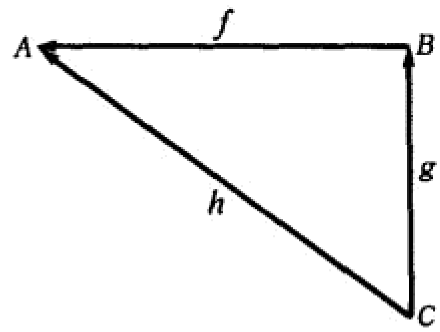


图 5-8

对偶范畴的作用在于它提供了极其重要的对偶原则。

设 S 是一个对任何范畴都有意义的陈述句(说明一个概念,提出一个命题,肯定一条规律等等),若 $S(\mathscr{C})$ 是 S 在范畴 $\mathscr{C}$ 上的具体体现,则 $S(\mathscr{C}^{OP})$ 是 S 在 $\mathscr{C}^{OP}$ 上的具体体现。

将 $S(\mathscr{C}^{OP})$ 中 $\mathscr{C}^{OP}$ 的对象换成 $\mathscr{C}$ 的对象,把 $\mathscr{C}^{OP}$ 中的态射换成 $\mathscr{C}$ 的态射(只需倒转箭头方向),这样就得到一个有关 $\mathscr{C}$ 的陈述句 $S^*(\mathscr{C})$,这个 $S^*(\mathscr{C})$ 叫 $S(\mathscr{C})$ 的对偶陈述句。如果 $S(\mathscr{C})$ 说明一个有关 $\mathscr{C}$ 的概念,则 $S^*(\mathscr{C})$ 说明一个有关 $\mathscr{C}$ 的对偶概念;如果 $S(\mathscr{C})$ 肯定有关 $\mathscr{C}$ 的一条规律,则 $S^*(\mathscr{C})$ 肯定一条有关 $\mathscr{C}$ 的对偶规律。这就是对偶原则。

我们再次强调,S 必须是一个对任何范畴都有意义的陈述句,此时 $S^*(\mathscr{C})$ 才有意义。若 S 是一条定理,并至少对 $\mathscr{C}$ 和 $\mathscr{C}^{OP}$ 都已证明,则 $S^*(\mathscr{C})$ 也是一条定理,无须再证,因为对偶原则本身已提供了证明。但要注意,运用对偶原则必须是对任何范畴都有意义的陈述句,否则不能运用,而必须另行证明,下面的定理将说明这个问题。

在 §5.1 中,我们已经定义了范畴中的同构的概念,我们再给出比同构较弱的概念。

定义 5.2.2 在范畴 $\mathscr{C}$ 中，若 $f \in \hom(A,B)$，$g \in \hom(B,A)$，且 $gf = 1_A$，则称 f 为 g 的截面态射，并称 g 为 f 的保核态射。

我们更感兴趣的是所谓满态射(epic)和单态射(monic)的概念。

定义 5.2.3 设 $\mathscr{C}$ 是一个范畴，$f \in \hom(A,B)$，若对 $\forall C \in \text{ob}\,\mathscr{C}$，$g_1, g_2 \in \hom(C,A)$，由 $fg_1 = fg_2 \Rightarrow g_1 = g_2$，则称 f 为单态射；若 $g_1, g_2 \in \hom(B,C)$，由 $g_1 f = g_2 f \Rightarrow g_1 = g_2$，则称 f 为满态射。

本定义中的满态射与单态射是对偶的，为了说明对偶原则的应用，我们赘述如下。

设 $S(\mathscr{C})$："由 $fg_1 = fg_2 \Rightarrow g_1 = g_2$，则 f 叫单态射。"

将 $\mathscr{C}$ 中的对象换成 $\mathscr{C}^{OP}$ 中的对象，实质上还是原来的对象，并将其箭头方向倒转过来，得

$S^*(\mathscr{C})$："由 $g_1 f = g_2 f \Rightarrow g_1 = g_2$，则 f 叫满态射。"

下列命题进一步说明了对偶原则的应用。

命题 5.2.1 令 $\mathscr{C}$ 是一个范畴，

(1) 若 $f \in \hom(A,B)$，$g \in \hom(B,C)$，f 和 g 都是单态射(满态射)，则 gf 也是单态射(满态射)。

(2) 若 gf 是单态射(满态射)，则 f 是单态射(g 是满态射)。

(3) 若 f 有截面态射，则 f 是满态射；若 f 有保核态射，则 f 是单态射。

证 (1) 设 $gfh_1 = gfh_2 \Rightarrow fh_1 = fh_2 \Rightarrow h_1 = h_2$，故 gf 是单态射。

(2) 设 $fh_1 = fh_2 \Rightarrow gfh_1 = gfh_2$，因 gf 是单态射，故 $h_1 = h_2$。

(3) 若 $f \in \hom(A,B)$，$g \in \hom(B,A)$，且 $gf = 1_A$，g 是 f 的保核态射，若 $fh_1 = fh_2 \Rightarrow gfh_1 = gfh_2 \Rightarrow h_1 = h_2$，故 f 是单态射。

由对偶原则,满态射的结论都应成立。

命题 5.2.2 在集范畴 **Set** 中,

(1)$f \in \hom_{Set}(A,B)$ 是单态射当且仅当 f 是单射;

(2)$f \in \hom_{Set}(A,B)$ 是满态射当且仅当 f 是满射。

证 由对偶原则,仅需证明关于单态射的结论。

必要性 若 f 不是单射,则 $\exists x_1 \neq x_2$ 使 $f(x_1) = f(x_2)$,令

$$h_1(f(x)) = x_1$$

$$h_2(f(x)) = \begin{cases} x_2, f(x) = f(x_2) \\ x, f(x) \neq f(x_2) \end{cases}$$

则 $h_1 \neq h_2$,但 $fh_1(f(x)) = fh_2(f(x)) \Rightarrow fh_1 = fh_2$,故 f 不是单态射。

充分性 若 f 不是单态射,则 $\exists h_1 \neq h_2, fh_1 = fh_2$,故 $\exists y_1 \neq y_2, h_1(x) = y_1, h_2(x) = y_2, fh_1(x) \neq fh_2(x)$,与 $fh_1 = fh_2$ 矛盾。

这个结论可以推广到群范畴 **Grp** 和 R- 模范畴 **R-Mod** 中。

定理 5.2.1 在群范畴 **Grp** 中,f 是单(满)态射的充要条件是 f 是单(满)同态。

证 因满同态与单同态不对偶,故本定理中满、单部分都需证明。

(1) 先证"单"的部分。

必要性 设 f 不是单同态,$f \in \hom(A,B)$,则 $C = \ker f \neq 1$,令 g 是 C 到 A 的单同态,使 $\forall x \in C, g(x) = x$,则 fg 是 C 到 B 的同态,且 $fg(x) = 1$,再令 h 是 C 到 A 的同态,使 $\forall x \in C$, $h(x) = 1$,显然 $fh(x) = 1$,且由 $C \neq 1 \Rightarrow g \neq h$,又由 $fg = fh \not\Rightarrow g = h$,$f$ 不是单态射。

充分性 设 f 是单同态,则 f 作为集合的映射是单射,故左消去律成立,即 $fg_1 = fg_2 \Rightarrow g_1 = g_2$,因此 f 是单态射。

(2) 次证定理中“满”的部分。

必要性　设 f 不是满同态，则 $f(A) \subsetneq B$，令 $C = f(A)$，若 $[B:C] = 2$，则 $C \triangleleft B$，做商群 B/C，显然 $B/C \neq 1$。

令

$$g: B \to B/C$$
$$x \to xC$$

是一个同态，再令

$$h: B \to B/C$$
$$x \to T \quad (T \text{ 为 } B/C \text{ 的单位元})$$

也是一个同态，显然 $g \neq h$，但 $gf = hf$，因 $\forall a \in A, f(a) \in C$，$gf(a) = g(f(a)) = T = hf(a)$，故 f 不是满态射，矛盾。

下设 $[B:C] > 2$，令

$$g: B \to \text{sym } B$$
$$b \to b_L: x \to bx$$

令 $h = kg$，其中 k 是 sym B 的内自同构，即

$$k: \text{sym } B \to \text{sym } B$$
$$y \to pyp^{-1}$$

此处，$y \in \text{sym } B$，p 为 sym B 的一个固定元。

因此，$h(b) = kg(b) = pb_L p^{-1}$。

又因和所有左平移映射 b_L 都可换的映射必为右平移映射，故若 p 不是右平移映射，有 $h = kg \neq g$。

因任取不等于1的平移没有不动点，故若 p 是不等于1的有不动点的置换，则 p 不是右平移，因而 $h \neq g$。

下面构造一个 p，使 p 是不等于1的有不动点的置换，且 p 与 d_L 可换($\forall d \in C$)，可推出 $hf = gf$。

令 σ 是右陪集空间 $B/C = \{Cb \mid b \in B\}$ 的置换，$\sigma \neq 1$ 且有不动点(因为 $|B/C| > 2$，这总可办到)。

令 I 是右陪集的代表元的集合,则 B 中每个元可以用惟一的方式写成积 $cu, c \in C, u \in I$。

若 $\sigma(cu) = cu'$,则定义 $p(cu) = cu'$,故 $p \in \mathrm{sym}\ B, p \neq 1$(因 $\sigma \neq 1$),σ 有不动点,故 p 有不动点,显然,p 与 d_L 可换,$\forall d \in C, \forall a \in A, f(a) \in C$,故 $p f(a)_L = f(a)_L p \Rightarrow f(a)_L = pf(a)_L p^{-1}$,即 $g(f(a)) = h(f(a)) \Rightarrow gf = hf$。

由 $hf = gf \Rightarrow h \neq g$,故 f 不是满态射。

充分性　若 f 是满同态,$f \in \mathrm{hom}(A, B)$,$\forall g, h \in \mathrm{hom}(B, C)$,若 $g \neq h$,则 $\exists b \in B$,使 $g(b) \neq h(b)$,又 f 是满同态,必 $\exists a \in A$,使 $f(a) = b$,故

$$gf(a) = g(f(a)) = g(b) \neq h(b) = h(f(a)) = hf(a)$$

因而 $gf \neq hf$,故 f 是满态射。

定理 5.2.2　环 R 上的模范畴 **R-Mod** 上的态射 f 是单态射(满态射)的充要条件是 f 是 R- 模的单同态(满同态)。

证　因 R- 模可看做一个加群,证明同定理 5.2.1 类似。

类似的定理在环范畴 **Ring** 中是否成立?我们有如下的结论。

定理 5.2.3　环范畴 **Ring** 的态射 f 是单态射当且仅当 f 是环的单同态,但却存在 **Ring** 的一个满态射,它不是满同态。

证　由上一个定理已证,f 是环 R 的单(满)同态时,f 是 **Ring** 的单(满)态射。

反之,若 f 是 **Ring** 的单态射,则不能采用上一个定理的证明方法,因理想不一定是环,即便是环,而同态核的单射也不一定是环的单同态,故采用与定理 5.2.2 不同的证明方法。

若 f 不是单同态,令

$$A \oplus A = \{(a_1, a_2) \mid a_i \in A\}$$

定义
$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$
$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2)$$

$$1 = (1,1)$$

则 $A \oplus A$ 是一个环。

令 $$K = \{(a_1,a_2) \mid f(a_1) = f(a_2)\} \leqslant A \oplus A$$

且 $K \supsetneqq D = \{(a,a) \mid a \in A\}$(因 f 非单同态，$\exists a_1 \neq a_2, f(a_1) = f(a_2)$)。

令 $$g_1: K \to A \qquad g_2: K \to A$$
$$(a_1,a_2) \to a_1 \qquad (a_1,a_2) \to a_2$$

由 K 的定义，$fg_1 = fg_2$，0 又 $K \supsetneqq D$，$\exists (a_1,a_2) \in K, a_1 \neq a_2 \Rightarrow g_1(a_1,a_2) = a_1 \neq a_2 = g_2(a_1,a_2) \Rightarrow g_1 \neq g_2$，故 f 非单态射，此为矛盾，故 f 必为单同态。

但 f 满态射时却不一定是满同态，现举反例如下：

令 $f: \mathbf{Z} \to \mathbf{Q}$，$f$ 是单同态，再令 $g: \mathbf{Q} \to \mathbf{R}$，$h: \mathbf{Q} \to \mathbf{R}$，$g, h$ 均是同态映射，则 $gf = hf \Leftrightarrow g|_{\mathbf{Z}} = h|_{\mathbf{Z}}$。故 $gf = hf \Rightarrow g = h$，因而 f 是满态射，f 不是满同态。

习题 5.2

1. 在 **Top** 范畴中给出一个例子，一个态射是单且满的，但没有保核态射。
2. 设 G 是一个有限群，H 是 G 的一个子群。证明，对 $h \in H$，同每个 h_L(作用在 G 上) 可换的 G 的置换个数是

$$[G:H]! \mid H \mid^{[G:H]}$$

此处 $[G:H]$ 是 H 在 G 中的指数。

§5.3 函子

我们先从一个实例引出函子的概念。

设 $R,S,T\in \mathrm{ob}\,\mathbf{Ring}$，$U(R),U(S),U(T)$ 分别表示 R,S,T 的可逆元构成的乘法群，显然，$U(R),U(S),U(T)\in \mathrm{ob}\,\mathbf{Grp}$。如果 f 是 R 到 S 的环同态，g 是 S 到 T 的环同态，则 $f|_{U(R)}$ 是 $U(R)$ 到 $U(S)$ 的群同态，$g|_{U(S)}$ 是 $U(S)$ 到 $U(T)$ 的群同态，且 $gf|_{U(R)}=(g|_{U(S)})\cdot(f|_{U(R)})$，$1_R|_{U(R)}$ 是 $U(R)$ 的恒等映射。

则由环到群的法则 $\eta:R\to U(R)$ 和环同态到群同态的映射 $\zeta:f\to f|_{U(R)}$ 就构成了由环范畴 **Ring** 到群范畴 **Grp** 的一个函子(functor)。

一般说来，从一个范畴 $\mathscr{C}$ 到另一个范畴 $\mathscr{D}$ 的函子可粗略地看成"映射"，它把 $\mathscr{C}$ 的任一对象映射成 $\mathscr{D}$ 的一个对象，把集合 $\hom_{\mathscr{C}}(A,B)$ 映射到集合 $\hom_{\mathscr{D}}(FA,FB)$，并且保持态射的乘积运算与恒等态射，故范畴 $\mathscr{C}$ 到范畴 $\mathscr{D}$ 的函子也可看做"同态"，我们给出函子的定义。

定义 5.3.1 令 $\mathscr{C}$ 和 $\mathscr{D}$ 是范畴，从 $\mathscr{C}$ 到 $\mathscr{D}$ 的一个函子 F 由下面两部分构成：

(1) $\forall A\in \mathrm{ob}\,\mathscr{C}$，均有 $FA\in \mathrm{ob}\,\mathscr{D}$；

(2) $\forall f\in \hom_{\mathscr{C}}(A,B)$，$A,B\in \mathrm{ob}\,\mathscr{C}$，均有

$$F(f)\in \hom_{\mathscr{D}}(FA,FB)$$

并且满足下面两个条件：

① $F(gf)=F(g)F(f)$；

② $F(1_A)=1_{F(A)}$。

在函子定义中，条件 ① 可用下列图形可换来表示。

在 $\mathscr{C}$ 中，$h=gf$ 可表为图 5-9；在 $\mathscr{D}$ 中，$F(h)=F(gf)=F(g)F(f)$ 可表为图5-10。确切地说，称定义 5.3.1 中的函子 F 为共变函子。

定义 5.3.2 称由 $\mathscr{C}^{op}$ 到 $\mathscr{D}$ 的一个共变函子 F 为 $\mathscr{C}$ 到 $\mathscr{D}$ 的反

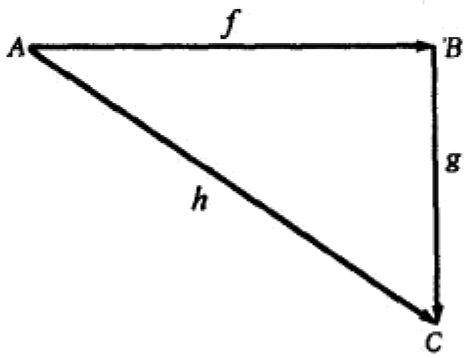


图 5-9

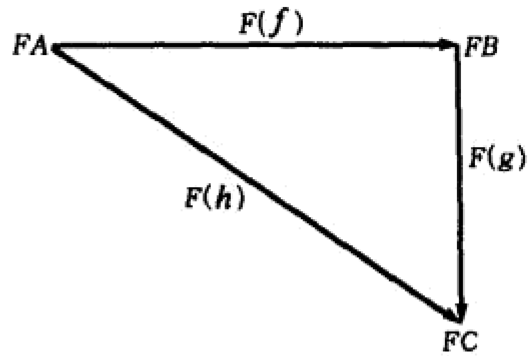


图 5-10

变函子，即 $\forall A \in \text{ob}\,\mathscr{C}$，均有 $FA \in \text{ob}\,\mathscr{D}$，且对 $\mathscr{C}$ 中任一对象对 (A,B)，存在映射

$$F:\hom_{\mathscr{C}}(A,B) \to \hom_{\mathscr{D}}(FB,FA)$$

使得

$$F(fg) = F(g)F(f)$$
$$F(1_A) = 1_{FA}$$

定义 5.3.3 设 $\mathscr{B},\mathscr{C},\mathscr{D}$ 是范畴，称由 $\mathscr{B}\times\mathscr{C}$ 到 $\mathscr{D}$ 的一个共变函子 F 为 $\mathscr{B}$ 和 $\mathscr{C}$ 到 $\mathscr{D}$ 的二变项函子；称由 $\mathscr{B}^{OP}\times\mathscr{C}$ 到 $\mathscr{D}$ 的共变函子为 $\mathscr{B}$ 中反变在 $\mathscr{C}$ 中共变的二变项函子；称由 $\mathscr{B}^{OP}\times\mathscr{C}^{OP}$ 到 $\mathscr{D}$ 的一个共变函子为在 $\mathscr{B}$ 和 $\mathscr{C}$ 中都反变的二变项函子。

请看一些例子。

例 1 设范畴 $\mathscr{D}$ 是范畴 $\mathscr{C}$ 的子范畴，J 是 $\mathscr{D}$ 到 $\mathscr{C}$ 的一个函子，$\forall A \in \text{ob}\,\mathscr{D}, JA = A \in \text{ob}\,\mathscr{C}, f \in \hom_{\mathscr{D}}(A,B), J(f) = f \in \hom_{\mathscr{C}}(A,B)$，称 J 是 $\mathscr{D}$ 到 $\mathscr{C}$ 的嵌入函子，特别地，当 $\mathscr{D}=\mathscr{C}$ 时，称 J 为恒等函子。

例 2 由 **Grp** 到 **Set** 的函子 F，$\forall G \in \text{ob}\,\mathbf{Grp}$，总有 G 的基础集 G（忘掉了它的代数结构的集）$\in$ **Set**，且 $\forall f \in \hom_{\mathbf{Grp}}(G,G')$，$f$ 是群同态，对应 $F(f)$ 是集的映射，即 $F(f) \in \hom_{\mathbf{Set}}(G,G')$，也忘掉了群同态的保持运算的性质，称 F 为忘却函子(forget functor)。例如 **Ring** 到 **Ab** 的忘却函子是忘掉了环中的乘法结构和

乘法同态，而 **Ring** 到 **Mon** 的忘却函子是忘掉了环中的加法结构和加法同态。

例 3 从 **Ring** 到 **Ring** 的函子 M_n：

(1) $\forall R \in \text{ob}\,\mathbf{Ring}$，令 $M_n(R) = \{(x_{ij})_{n\times n} \mid x_{ij} \in R, n \in \mathbf{Z}^+\}$，则 $M_n(R) \in \text{ob}\,\mathbf{Ring}$；

(2) $\forall f \in \text{hom}_{\mathbf{Ring}}(R,S)$，则

$$M_n(f): M_n(R) \to M_n(S)$$
$$(x_{ij}) \to (f(x_{ij}))$$

则 $M_n(f) \in \text{hom}_{\mathbf{Ring}}(M_n(R), M_n(S))$。

例 4 从 **Ring** 到 **Grp** 的函子 G_{L_n}：

(1) $\forall R \in \text{ob}\,\mathbf{Ring}$，令 $G_{L_n}(R)$ 为 $M_n(R)$ 中的逆阵构成的群，则 $G_{L_n}(R) \in \mathbf{Grp}$；

(2) $\forall f \in \text{hom}_{\mathbf{Ring}}(R,S)$，$G_{L_n}(f) \in \text{hom}_{\mathbf{Grp}}(G_{L_n}(R), G_{L_n}(S))$。

例 5 从 **Set** 到 **Set** 的幂函子 $\mathscr{P}$：

(1) $\forall A \in \text{ob}\,\mathbf{Set}$，有 $\mathscr{P}(A) \in \text{ob}\,\mathbf{Set}$；

(2) $\forall f \in \text{hom}_{\mathbf{Set}}(A,B)$，令

$$\mathscr{P}(f) \triangleq f_{\mathscr{P}}: \mathscr{P}(A) \to \mathscr{P}(B)$$
$$A_1 \to f_{\mathscr{P}}(A_1) \triangleq f(A_1)$$

故 $\mathscr{P}(f) \in \text{hom}_{\mathbf{Set}}(\mathscr{P}(A), \mathscr{P}(B))$。

例 6 从 **Grp** 到 **Ab** 的交换化函子 A：

设 $G \in \text{ob}\,\mathbf{Grp}$，$(G,G) = \langle\{aba^{-1}b^{-1}\}\rangle$ 为换位子群，则

$$G/(G,G) \in \text{ob}\,\mathbf{Ab}, A(G) = G/(G,G)$$

$\forall f \in \text{hom}_{\mathbf{Grp}}(G,H)$，则由 $f((G,G)) = (H,H)$ 导出

$$A(f) \triangleq f^* : G/(G,G) \to H/(H,H)$$

例 7 设 **Poset** 为对象是偏序集的范畴，其态射为保序映射，

由 **R-Mod** 到 **Poset** 的函子 L 如下定义：

(1) $\forall M \in \text{ob}\,\mathbf{R\text{-}Mod}$，$L(M)$ 是由包含关系决定的 M 的子模的基础集，则 $L(M) \in \text{ob}\,\mathbf{Poset}$；

(2) 若 $f \in \hom_{\mathbf{R\text{-}Mod}}(M,N)$，由 f 决定 $L(M)$ 到 $L(N)$ 的一个保序映射 $L(f)$，则 $L(f) \in \hom_{\mathbf{Poset}}(L(M),L(N))$。

例 8 投影函子 P：

设 $\mathscr{C}\times\mathscr{D}$ 是积范畴，$\forall (A,B) \in \text{ob}\,\mathscr{C}\times\mathscr{D}$，$\exists P(A,B) = A \in \text{ob}\,\mathscr{C}$，$\forall (f,g) \in \hom((A,B),(A',B'))$，$P(f,g) = f \in \hom(A,A')$。

例 9 对角函子 D：

$\forall A \in \text{ob}\,\mathscr{C}$，$D(A) = A \times A \in \text{ob}\,\mathscr{C}\times\mathscr{C}$，$\forall f \in \hom_{\mathscr{C}}(A,B)$，$D(f) = (f,f) \in \hom_{\mathscr{C}\times\mathscr{C}}((A,A),(B,B))$。

例 10 由 **R-Mod** 到 **Mod-R** 的反变函子 D：

$\forall M \in \text{ob}\,\mathbf{R\text{-}Mod}$，令 $M^* = \hom_{\mathbf{R\text{-}Mod}}(M,R)$，在 M^* 中定义

$$(f+g)(x) = f(x) + g(x)$$
$$(fs)(x) = f(x)s, \forall x \in M, s \in R$$

则 M^* 是右 R- 模，即 $M^* \in \text{ob}\,\mathbf{Mod\text{-}R}$。令 $D(M) = M^*$，$\forall L \in \hom_{\mathbf{R\text{-}Mod}}(M,N)$，$g \in \hom_{\mathbf{R\text{-}Mod}}(N,R)$，由 g 与 L 的合成 gL 定义一个转置映射

$$L^* : N^* \to M^*$$
$$g \to gL$$

显然 $L^* \in \hom_{\mathbf{Mod\text{-}R}}(N^*,M^*)$。

如果 $M_1 \xrightarrow{L_1} M_2 \xrightarrow{L_2} M_3$，$\forall g \in M_3^*$，则

$$(L_2L_1)^*(g) = gL_2L_1 = (gL_2)L_1 = L_1^*L_2^*(g)$$

故 $(L_2L_1)^* = L_1^*L_2^*$。

显然有 $(1_M)^* = 1_{M^*}$。

令 $D(L) = L^*$，D 是一个反变函子。显然，函子具有保同构

的性质，即若 f 是范畴 $\mathscr{C}$ 的同构态射，$fg = 1_B$，$gf = 1_A$，又 F 是 $\mathscr{C}$ 到 $\mathscr{D}$ 的函子，则

$$F(f)\cdot F(g) = 1_{FB}, F(g)\cdot F(f) = 1_{FA}$$

即 $F(f)$ 是 $\mathscr{D}$ 的同构态射，类似的结论对截面态射和保核态射均成立，但有反例说明(习题 5.3)，对满态射和单态射不成立。

下面讨论函子的合成。

定义 5.3.4 若 F 是范畴 $\mathscr{C}$ 到 $\mathscr{D}$ 的函子，G 是范畴 $\mathscr{D}$ 到 $\mathscr{F}$ 的函子，定义

$$(GF)A = G(FA), \forall A \in \text{ob}\,\mathscr{C}$$
$$(GF)(f) = G(F(f)), \forall f \in \hom_{\mathscr{C}}(A,B)$$

则称由 $\mathscr{C}$ 到 $\mathscr{F}$ 的函子 GF 为 F 与 G 的合成。

类似地，我们还可以定义两个反变函子的合成及一个反变函子与一个共变函子的合成。若 F 和 G 中有一个是反变函子而另一个是共变函子，其合成将是反变函子；若 F，G 都是反变函子，则合成必为共变函子。

定义 5.3.5 一个函子 F 称为一一的(完全的)，如果对 $\mathscr{C}$ 中每一对(A,B)，映射

$$F:\hom_{\mathscr{C}}(A,B) \to \hom_{\mathscr{D}}(FA,FB)$$
$$f \to F(f)$$

是单射(满射)。

如果 F 既是一一的，又是完全的，称为一一完全函子。

在例1中，嵌入函子是一一完全函子的充要条件是 $\mathscr{D}$ 是 $\mathscr{C}$ 的完满的子范畴。

在例 2 中的忘却函子是一一的，但不是完全的。

在例 8 中的投影函子是完全的，但不是一一的。

下面给出两个函子之间的重要概念 —— 自然变换。

定义 5.3.6 设 F，G 为范畴 $\mathscr{C}$ 到 $\mathscr{D}$ 的函子，定义 F 到 G 的自然变换 η 如下：

$\forall A \in \mathrm{ob}\,\mathscr{C}$,指定 $\eta_A \in \hom_{\mathscr{D}}(FA, GA)$,使得对 $\forall A, B \in \mathrm{ob}\,\mathscr{C}$, $\forall f \in \hom_{\mathscr{C}}(A, B)$,下面的矩形(图 5-11) 是可换的,即

$$G(f) \cdot \eta_A = \eta_B \cdot F(f)$$

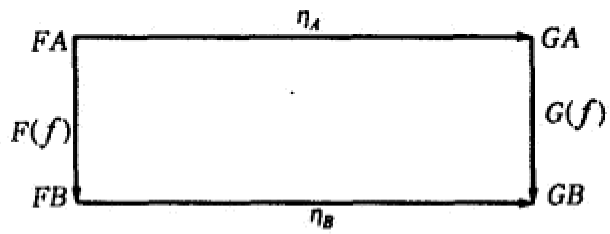


图 5-11

特别地,若对每一个 η_A 是同构的,则称 η 是自然同构。

现在考虑本章开头所述之例子,并将它一般化。

设 **R-Mod** 是环 R 上的左 R- 模,$\forall M \in \mathrm{ob}$ **R-Mod**,令 $M^* = \hom(M, R)$,$M^{**} = \hom(M^*, R)$,显然,$M^{**} = (M^*)^*$。

D 是 **R-Mod** 到 **Mod-R** 的反变函子,故

$$M \xrightarrow{D} M^* \xrightarrow{D} (M^*)^* = M^{**}$$

因而 $M \xrightarrow{D^2} M^{**}$,$D^2$ 是 **R-Mod** 到自身的共变函子,我们称之为重对偶函子。

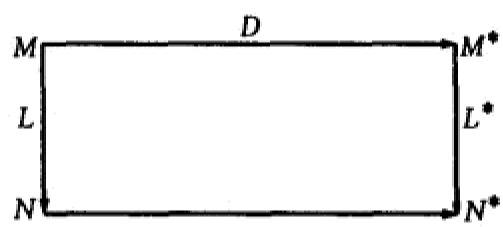


图 5-12

$\forall L \in \hom_{\mathscr{C}}(M, N)$,$D^2(L) \triangleq L^{**} \in \hom_{\mathscr{C}}(M^{**}, N^{**})$,$\forall x \in M$,$g \in N^*$,由例 10(参见图 5-12),则 $L^* g \in M^*$,且 $(L^* g)(x) = g(Lx)$,再次运用反变函子,$\forall \varphi \in M^{**}$,$L^{**}\varphi \in N^{**}$,且$(L^{**}\varphi)(g) = \varphi(L^* g)$,$\forall f \in M^*$,$x \in M$,令

$$\eta_M(x): M^* \to R$$

$$f \to f(x)$$

$\eta_M(x) \in M^{**} = \hom(M^*, R)$，故 $\eta_M \in \hom(M, M^{**})$。

又 $Lx \in N$，令

$$\eta_N(Lx): N^* \to R$$
$$g \to g(Lx)$$

故 $\eta_N(Lx) \in N^{**}$，因而有

$$L^{**}\eta_M(x)(g) =$$
$$\eta_M(x)(L^* g) =$$
$$L^*(g(x)) =$$
$$gL(x) = \eta_N(Lx)(g)$$

故 $L^{**}\eta_M(x) = \eta_N L(x)$，$\forall x \in M$，因而

$$L^{**}\eta_M = \eta_N L$$

这表示下面的矩形(图 5-13)是可换的。

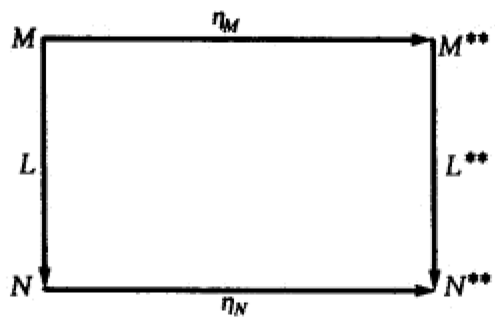


图 5-13

现在令 $I_{\mathbf{R\text{-}Mod}}$ 是 **R-Mod** 的恒等函子，D^2 是 **R-Mod** 的重对偶函子，$\forall M \in \text{ob}\,\mathbf{R\text{-}Mod}$，指定 $\eta_M \in \hom_{\mathbf{R\text{-}Mod}}(M, M^{**})$，由上面的讨论得到图 5-14，故 η 是由 $I_{\mathbf{R\text{-}Mod}}$ 到 D^2 的自然变换。

再请看两个自然变换的例子。

例 11 在 **R-Mod** 中定义函子 $\oplus_n$，$\forall M \in \text{ob}\,\mathbf{R\text{-}Mod}$，令

$$\oplus_n M \triangleq M^{(n)} = \{(a_1, a_2, \cdots, a_n) \mid a_i \in M, i = 1, 2, \cdots, n\}$$

$\forall f \in \hom(M, N)$，令

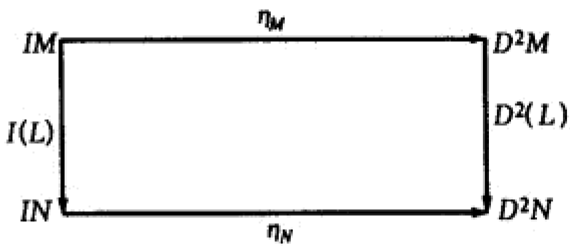


图 5-14

$$\oplus_n f \triangleq f^{(n)}:(a_1,a_2,\cdots,a_2)\to(f(a_1)f(a_2),\cdots,f(a_n))$$

再定义一个对角同态，$\forall M\in$ ob **R-Mod**，令

$$\delta_M^{(n)}:M\dashrightarrow M^{(n)}$$

$$a\to(a,a,\cdots,a)$$

则 $\delta_M^{(n)}$ 是由恒等函子 $I_{\mathbf{R\text{-}Mod}}$ 到 $\oplus_n$ 的一个自然变换，因为下图(图 5-15)可换。

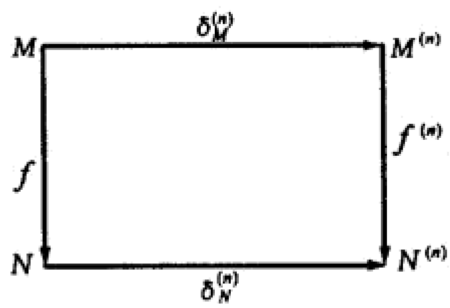


图 5-15

例 12 设群范畴 **Grp** 的交换化函子 A 是由 **Grp** 到 **Grp** 的函子，而不是 **Grp** 到 **Ab** 的函子，这只需扩大上域就可办到。

$\forall G\in$ ob **Grp**，令

$$\gamma_G:G\to G/(G,G)$$

$$a\to a(G,G)$$

则有图形(图 5-16)可换。γ 是由 $I_{\mathbf{Grp}}$ 到 A 的自然变换。

下面给出两个自然变换的积的定义。

定义 5.3.7 令 F,G,H 都是范畴 $\mathscr{C}$ 到 $\mathscr{D}$ 的函子，η 是 F 到 G 的自然变换，ζ 是 G 到 H 的自然变换，$\forall A\in$ ob $\mathscr{C}$，则 $\eta_A\in$

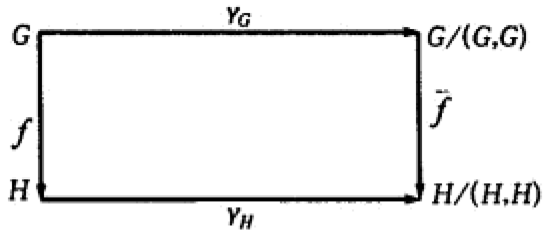


图 5-16

$\hom_{\mathscr{D}}(FA,GA)$，$\zeta_A \in \hom_{\mathscr{D}}(GA,HA)$，故 $\zeta_A\eta_A \in \hom_{\mathscr{D}}(FA,HA)$，且下面的图形(图 5-17)由两个小矩形的可换可得大矩形可换：

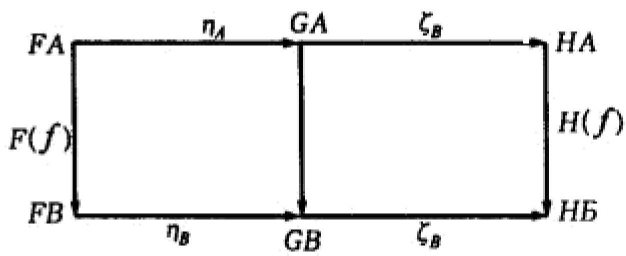


图 5-17

故 $\zeta\eta$ 是 F 到 H 的自然变换，称为 ζ 与 η 的积。

虽然，若 F 是范畴 $\mathscr{C}$ 到 $\mathscr{D}$ 的函子，则可得由 F 到 F 的自然变换 I_F，设 G 是 $\mathscr{C}$ 到 $\mathscr{D}$ 的另一个函子，并设 η 是 F 到 G 的任一自然变换，则有 $\eta I_F = \eta = I_G\eta$。

我们也有自然变换的逆变换的定义。

定义 5.3.8 设 η 是由函子 F 到 G 的自然变换，ζ 是由 G 到 F 的自然变换，使得 $\zeta\eta = I_F$ 且 $\eta\zeta = I_G$，则 η 是自然同构，ζ 是 η 的逆变换，记做 $\eta^{-1} = \zeta$。

如果 η 是由 $\mathscr{C}$ 到 $\mathscr{C}$ 的函子 E 到恒等函子 $I_{\mathscr{C}}$ 的自然同构，则由图 5-18 的可换性，可得 $E(f) = \eta_B f \eta_A^{-1}$，由此可得

$$E:\hom(A,B) \to \hom(E_A,E_B)$$
$$f \to E(f)$$

是双射。

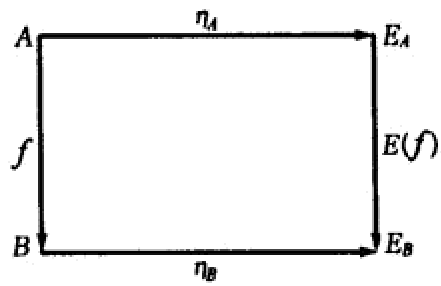


图 5-18

习题 5.3

1. 设 F 是从 $\mathscr{C}$ 到 $\mathscr{D}$ 的函子且 F 是一一完全的，$f \in \hom_{\mathscr{C}}(A,B)$。证明，下面的任何一个 $F(f)$ 的性质可推出 f 具有同样的性质：$F(f)$ 是满态射、单态射、有截面态射、有保核态射及 $F(f)$ 是同构的。
2. 设 M,N 是亚群，并把它们视为具有单个对象的范畴。证明：函子是一个 M 到 N 的同态，且一个函子 F 到一个函子 G 的自然变换对应于一个元素 $b \in N$，使得 $b(Fx) = (Gx)b, \forall x \in M$。
3. 使用第 2 题来构造一个函子 F 和一个满态射（单态射）f，使得 $F(f)$ 不是满态射（单态射）。
4. 设 G 是一个群，视 **G** 为一个对象的范畴。证明：从 **G** 到 **Set** 的一个函子和 G 到集合 S 的置换群 sym S 的同态一样，或者说，和 G 对 S 的作用一样；并证明两个这样的函子是自然同构当且仅当 G 的作用是等价的。
5. 设 $\mathscr{B},\mathscr{C},\mathscr{D},\mathscr{T}$ 是范畴，F,G 是从 $\mathscr{C}$ 到 $\mathscr{D}$ 的函子，K 是从 $\mathscr{C}$ 到 $\mathscr{C}$ 的函子，H 是从 $\mathscr{D}$ 到 $\mathscr{T}$ 的函子。证明：若 η 是从 F 到 G 的自然变换，则 $A \to H\eta_A$ 是 HF 到 HG 的自然变换，其中 $A \in \text{ob}\,\mathscr{C}$，$B \to \eta_{KB}$ 是从 FK 到 GK 的自然变换，其中 $B \in \text{ob}\,\mathscr{B}$。

6. 定义范畴$\mathscr{C}$的中心是$I_{\mathscr{C}}$到$I_{\mathscr{C}}$的自然变换的类，设$\mathscr{C}$ = **R-Mod**，c是R中心的元素，对$\forall M \in$ ob **R-Mod**，设$\eta_M(c)$是映射$x \to cx, x \in M$。证明：$\eta(c) M \to \eta_M(c)$在$\mathscr{C}$的中心内，且$\mathscr{C}$的中心的每个元素都具有这样的形式，再证明$c \to \eta(c)$是双射，因而**R-Mod**的中心是一个集合。

§5.4 范畴的等价性

定义 5.4.1 如果存在函子$F:\mathscr{C} \to \mathscr{D}$和$G:\mathscr{D} \to \mathscr{C}$，使得$GF = I_{\mathscr{C}}$和$FG = I_{\mathscr{D}}$，称范畴$\mathscr{C}$和$\mathscr{D}$同构。

这个定义相当强，以至于在许多情形下，同构的范畴都是等同的。因此，有必要将范畴同构的概念加点限制，放宽它的要求，故有下面的定义。

定义 5.4.2 如果存在函子$F:\mathscr{C} \to \mathscr{D}$和$G:\mathscr{D} \to \mathscr{C}$，使得$GF \cong I_{\mathscr{C}}, FG \cong I_{\mathscr{D}}$，此处"$\cong$"表示函子的自然同构，称范畴$\mathscr{C}$和$\mathscr{D}$等价。

显然，$\mathscr{C}$与$\mathscr{D}$同构$\Rightarrow$$\mathscr{C}$与$\mathscr{D}$等价，并且等价也是一种等价关系，即满足自反性、传递性、对称性。

注意，在定义 5.4.2 中，由F决定的G不是惟一的。

由函子对(F, G)给出了等价性，即$GF \cong I_{\mathscr{C}}, FG \cong I_{\mathscr{D}}$，由$GF \cong I_{\mathscr{C}}$，可推出映射

$$\begin{aligned} GF: \hom_{\mathscr{C}}(A, B) &\to \hom_{\mathscr{C}}(GFA, GFB) \\ f &\to GF(f) \end{aligned}$$

是双射，同理

$$\begin{aligned} FG: \hom_{\mathscr{D}}(A', B') &\to \hom_{\mathscr{D}}(FGA', FGB') \\ g &\to FG(g) \end{aligned}$$

也是双射。

进一步，由 GF 的单射可推出

$$F:\hom_{\mathscr{C}}(A,B)\to \hom_{\mathscr{D}}(FA,FB)$$
$$f\to F(f)$$

是单射，再由 FG 是满射可得 F 是满射，故 F 是一一完全的。

我们还注意到，$\forall A'\in \mathrm{ob}\,\mathscr{D}$，由 $FG\cong I_{\mathscr{D}}$ 给出同构函子 $\eta_{A'}\in \hom_{\mathscr{D}}(A',FGA')$，因此，若令 $A=GA'\in \mathrm{ob}\,\mathscr{C}$，则存在一个同构包含在 $\hom_{\mathscr{D}}(A',FA)$ 或 $\hom_{\mathscr{D}}(FA,A')$ 中。

定理 5.4.1 令 F 是范畴 $\mathscr{C}$ 到 $\mathscr{D}$ 的函子，存在 $\mathscr{D}$ 到 $\mathscr{C}$ 的函子 G，则 (F,G) 使 $\mathscr{C},\mathscr{D}$ 等价的充要条件是 F 是一一完全的，且 $\forall A'\in \mathrm{ob}\,\mathscr{D}$，$\exists A\in \mathrm{ob}\,\mathscr{C}$，使 FA 和 A' 在 $\mathscr{D}$ 中同构，即存在一个同构被包含在 $\hom_{\mathscr{D}}(FA,A')$ 中。

证 必要性前面已证，下面证充分性。

$\forall A'\in \mathrm{ob}\,\mathscr{D}$，选 $A\in \mathrm{ob}\,\mathscr{C}$，使 FA 与 A' 在 $\mathscr{D}$ 中同构。选定一个同构 $\eta_{A'}:A'\to FA$，定义 G：$\forall A'\in \mathrm{ob}\,\mathscr{D}$，有 $GA'\in \mathrm{ob}\,\mathscr{C}$，则 $\eta_{A'}:A'\to FGA'$；再取 $B'\in \mathrm{ob}\,\mathscr{D}$，令 $f'\in \hom(A',B')$，因 η_A 是同构，则存在惟一的 $\eta_{B'}f'\eta_{A'}^{-1}:FGA'\to FGB'$，使图 5-19 可换。

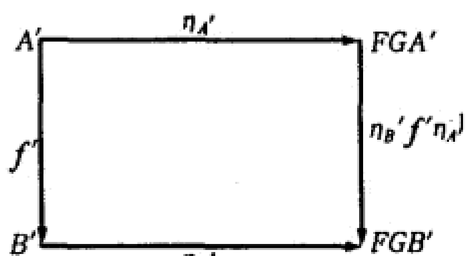


图 5-19

又因 F 是一一完全的，$\exists!\, f\in \hom_{\mathscr{C}}(GA',GB')$，使

$$F(f)=\eta_{B'}f'\eta_{A'}^{-1}$$

定义

$$G:\hom_{\mathscr{D}}(A',B')\to \hom_{\mathscr{C}}(GA',GB')$$
$$f'\to f$$

则 $\exists ! G(f') \in \hom_{\mathscr{C}}(GA', GB')$，使图 5-20 可换。

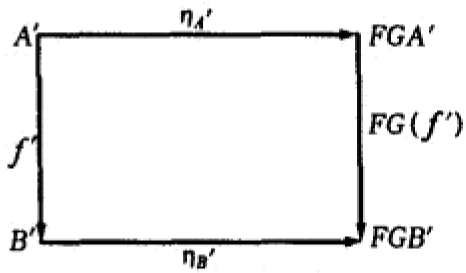


图 5-20

现令 $g' \in \hom_{\mathscr{D}}(B', C')$，则图 5-21 由两个小矩形可换可得大矩形可换。

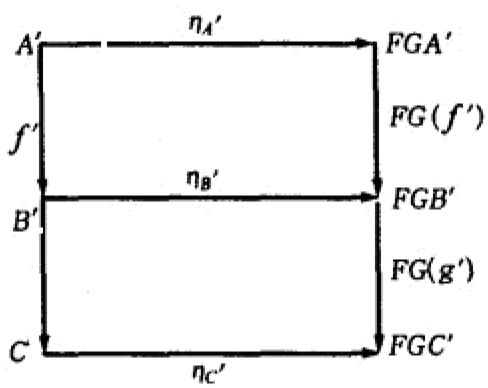


图 5-21

又因 F 是函子，有图 5-22 可换。

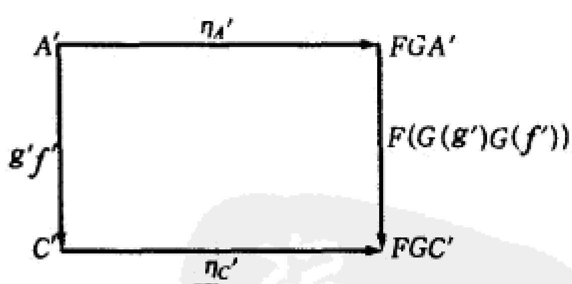


图 5-22

另一方面，有下面的矩形（图 5-23）可换，且 $G(g'f') \in \hom(GA', GC')$ 是上图中图形可换的惟一的态射。故

$$G(g')G(f') = G(g'f')$$

同理，$G(I_{A'}) = I_{GA'}$，故 G 是由 $\mathscr{D}$ 到 $\mathscr{C}$ 的一个函子，且由图 5-20 的可换性得出，η 是 I_{D} 到 FG 的自然同构。

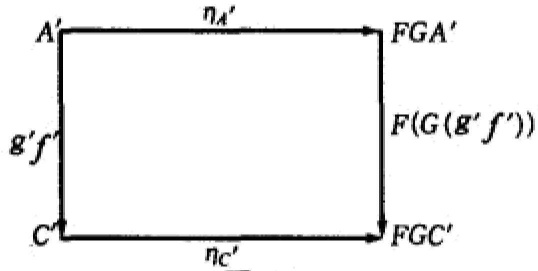


图 5-23

下面证明(F,G)使$\mathscr{C}$与$\mathscr{D}$等价。因已知$FG\cong I_{\mathscr{D}}$,只需证$GF\cong I_{\mathscr{C}}$,因F是一一完全的,可由$f'\in \hom(FA,FB)$是同构证得满足$F(f)=f'$的f也是同构(习题5.3第1题)。由

$$\eta_{FA}:FA\rightarrow FGFA$$

同构,则存在惟一的同构$\zeta_A:A\rightarrow GFA$,使得

$$F(\zeta_A)=\eta_{FA}$$

由图5-20的可换性,$A'=FA,B'=FB,f'=F(f)$,此处

$$f\in \hom(A,B)$$

可以推出下面的矩形(图5-24)可换。

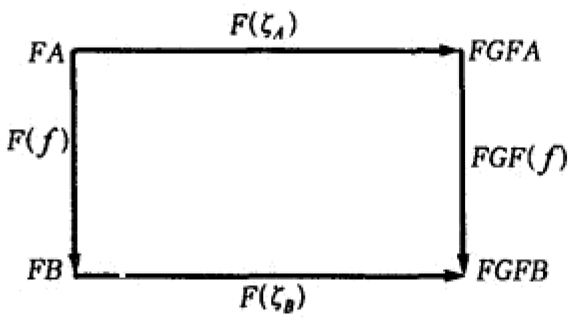


图 5-24

因F是一一的,又可推出下面图形(图5-25)可换,故ζ是$I_{\mathscr{C}}$到GF的自然同构,即(F,G)使$\mathscr{C}$与$\mathscr{D}$等价。

运用定理5.4.1,可得下面一个有趣的定理。

定理 5.4.2 令R是一个环,$M_n(R)=\{(r_{ij})_{n\times n}\mid r_{ij}\in R\}$,则 **Mod-R** 与 **Mod-M$_n$(R)** 等价。

证 设M是右R-模,$M^{(n)}=\{(x_1,x_2,\cdots,x_n)\mid x_i\in M,$

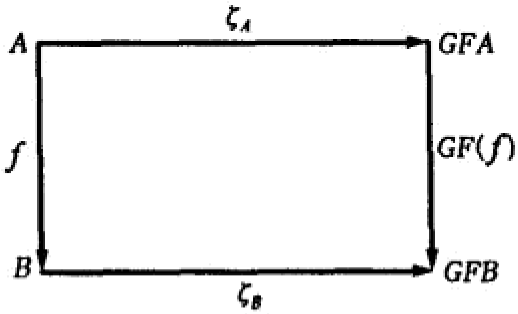


图 5-25

$i=1,2,\cdots,n\}$，$\mathbf{A}=(a_{ij})_{n\times n}\in M_n(R)$，其中 $a_{ij}\in R$，且 $M_n(R)$ 是一个环，定义

$$x\mathbf{A}=(x_1,x_2,\cdots,x_n)\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}=(y_1,y_2,\cdots,y_n)$$

此处 $y_i=\sum_{j=1}^{n}x_ja_{ji}\in M$，$i=1,2,\cdots,n$，则 $M^{(n)}$ 是一个右 $M_n(R)$-模。

令 $\forall M\in \text{ob}\ \mathbf{Mod\text{-}R}$，有 $M^{(n)}\in \text{ob}\ \mathbf{Mod\text{-}M_n(R)}$，使

$$F(M)=M^{(n)}$$

若 $f\in \hom_{\mathbf{Mod\text{-}R}}(M,N)$，取 $F(f)=f^{(n)}$，则

$$f^{(n)}:(x_1,x_2,\cdots,x_n)\to(f(x_1),f(x_2),\cdots,f(x_n))$$

$$f^{(n)}\in \hom_{\mathbf{Mod\text{-}M_n(R)}}(M^{(n)},N^{(n)})$$

故 F 是由 **Mod-R** 到 **Mod-M$_n$(R)** 的函子。下面证明 F 满足定理5.4.1的条件，则两个范畴 **Mod-R** 与 **Mod-M$_n$(R)** 的等价性就得到证明。

(1) 显然，F 是一一的。因为 $\forall f,g$，$f\neq g$，$\exists x_0$，$f(x_0)\neq g(x_0)\Rightarrow F(f)(x_0,\cdots,x_0)=(f(x_0),\cdots,f(x_0))\neq(g(x_0),\cdots,g(x_0))=F(g)(x_0,\cdots,x_0)\Rightarrow F(f)\neq F(g)$，故 $F(f)=f^{(n)}$ 是

单射。

(2) 再证 F 是完全的。令 $g \in \hom_{\mathbf{Mod\text{-}M_n(R)}}(M^{(n)}, N^{(n)})$，则 $M^{(n)}e_{11} = \{(x,0,\cdots,0) \mid x \in M\}$，此处，$e_{11}$ 表示第1行第1列元素是1，其余元素全是0的 n 阶方阵。

$N^{(n)}e_{11} = \{(y,0,\cdots,0) \mid y \in M\}$，因 g 是右 $M_n(R)$-模同态，故

$$g(M^{(n)}e_{11}) \subset N^{(n)}e_{11}$$

因而定义 $g(x,0,\cdots,0) = (f(x),0,\cdots,0)$，由 $g((x,0,\cdots,0)a') = (g(x,0,\cdots,0))a'$，得

$$f(x+y) = f(x) + f(y), f(xa) = f(x)a, a \in R$$

故 $f \in \hom_{\mathbf{Mod\text{-}R}}(M,N)$。

现由 $(x,0,\cdots,0)e_{1i} = (0,\cdots,0,x,0,\cdots,0)$，得

$$g((x,0,\cdots,0)e_{1i}) = g((0,\cdots,0,x,0,\cdots,0))$$

故 $g(0,\cdots,0,x,0,\cdots,0) = (0,\cdots,0,f(x),0,\cdots,0)$。因此有 $g = f^{(n)}$，即 F 是完全的。

(3) $\forall M' \in \text{ob}\,\mathbf{Mod\text{-}M_n(R)}$，往证 $\exists M \in \text{ob}\,\mathbf{Mod\text{-}R}$，使 $FM \cong M'$。令

$$F: R \to M_n(R)$$
$$a \to \text{diag}\{a,a,\cdots,a\} \triangleq a'$$

显然 F 是同态。

又因 M' 是右 $M_n(R)$-模，定义 $x'a \triangleq x'a', x' \in M'$，则 M' 是右 R-模。$a'e_{11} = e_{11}a' \triangleq e_{11}a$，故 $M = M'e_{11}$ 是 M' 的 R-子模。进一步，$\forall i = 1,2,\cdots,n, x'e_{i1} = x'e_{i1}e_{11} \in M$，故可定义

$$\eta_M : M' \to FM = M^{(n)}$$
$$x' \to (x'e_{11}, x'e_{21}, \cdots, x'e_{n1})$$

直接可以验证 η_M 是 $M_n(R)$-模同态。

若 $x'e_{i1}=0, 1\leqslant i\leqslant n$，则 $x'=\sum x'e_{ii}=\sum x'e_{i1}e_{1i}=0$，故 η_M 是单射。

又 $\forall(x_1,x_2,\cdots,x_n)\in M^{(n)}$，则 $x_i=x_i'e_{11}=(x_i'e_{1i})e_{i1}$，且

$$
\begin{aligned}
(x_1,x_2,\cdots,x_n)=&((x_1'e_{11})e_{11},(x_1'e_{11})e_{21},\cdots,(x_1'e_{11})e_{n1})+\\
&((x_2'e_{12})e_{11},(x_2'e_{12})e_{21},\cdots,(x_2'e_{12})e_{n1})+\\
&\cdots
\end{aligned}
$$

故 η_M 是满射，因此 η_M 是同构，即 $FM\cong M'$。

习题 5.4

1. 设 (F,G) 是 $\mathscr{C}$ 到 $\mathscr{D}$ 的一个等价，设 $f\in\hom_{\mathscr{C}}(A,B)$，证明：下面任何一个 f 的性质都导出 $F(f)$ 有同样的性质，即 f 是满态射、单态射，f 有截面态射，f 是同构的。
2. 对 $n>1$，范畴 **Mod-R** 和范畴 **Mod-M$_n$(R)** 同构吗？

§5.5　积和上积

在第 2 章中，我们已知，设 $G=G_1\times G_2$，G_i 是群，$i=1,2$，称 G 是 G_1 和 G_2 的直积群。令

$$
\begin{aligned}
P_i:G&\to G_i\\
(g_1,g_2)&\to g_i
\end{aligned}
$$

则 $P_i(i=1,2)$ 是 G 到 G_i 的投影同态。

设 H 为另一个群，并令 $f_i(i=1,2)$ 是 H 到 G_i 的群同态，则

$$
\begin{aligned}
f:H&\to G\\
h&\to f(h)=(f_1(h),f_2(h))
\end{aligned}
$$

是 H 到 G 的群同态，且 $P_if=f_i$，满足此条件的 f 是惟一的。(因若还有 f' 满足 $P_if'=f_i$，则 $f'(h)=(P_1f'(h),P_2f'(h))=$

$(f_1(h), f_2(h)) = f(h)$，故 $f' = f$)

群中的这个结论，可以推广到任意范畴中。

定义 5.5.1 设 $\mathscr{C}$ 是一个范畴，$A_1, A_2 \in \mathrm{ob}\,\mathscr{C}$，称 (A, P_1, P_2) 为 $\mathscr{C}$ 中的积，其中，$A \in \mathrm{ob}\,\mathscr{C}$，$P_i \in \hom_{\mathscr{C}}(A, A_i)$，$i = 1,2$，如果 $B \in \mathrm{ob}\,\mathscr{C}$，而 $f_i \in \hom_{\mathscr{C}}(B, A_i)$，$i = 1,2$，则存在惟一的 $f \in \hom_{\mathscr{C}}(B, A)$，使下面两个三角形（图 5-26 和图 5-27）都可换。

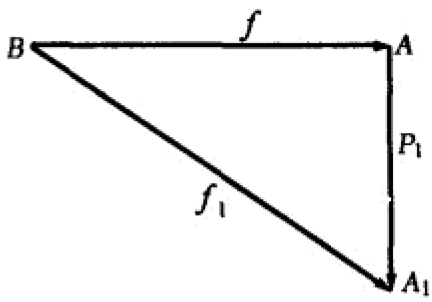


图 5-26

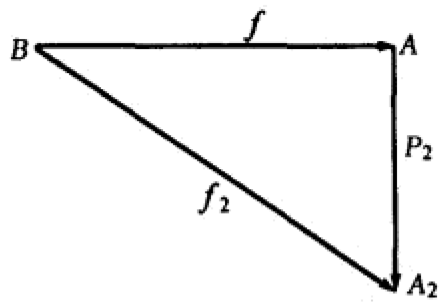


图 5-27

下面的命题保证了这样定义的积是惟一的。

命题 5.5.1 设 (A, P_1, P_2) 和 (A', P_1', P_2') 是 $\mathscr{C}$ 中对象 A_1, A_2 的积，则存在惟一的同构 $h: A \to A'$，使得

$$P_i = P_i' h, \qquad i = 1,2$$

证 由于 (A', P_1', P_2') 是 $\mathscr{C}$ 中对象 A_1, A_2 的积，又因为 $A \in \mathrm{ob}\,\mathscr{C}$，由定义 5.4.1，$\exists !h \in \hom(A, A')$，使得下面的图形（图 5-28）可换，即 $P_i = P_i' h$，$i = 1,2$。

同理，由 (A, P_1, P_2) 是 A_1, A_2 的积，有下面的图形（图 5-29）可换。即 $P_i' = P_i h$，$i = 1,2$。代入后得，$P_i' = P_i' h h'$，$P_i = P_i h' h$。

令 $A = A'$，再由定义 5.4.1，显然有下面的两个三角形（图 5-30）都是可换的。即 $P_i = P_i \cdot 1_A$，$P_i' = P_i' \cdot 1_{A'}$，且这样的 1_A，$1_{A'}$ 是惟一的，故

$$h'h = 1_A, \quad hh' = 1_{A'}$$

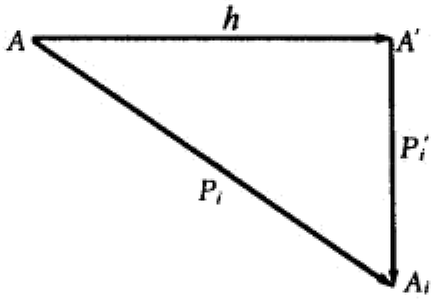


图 5-28

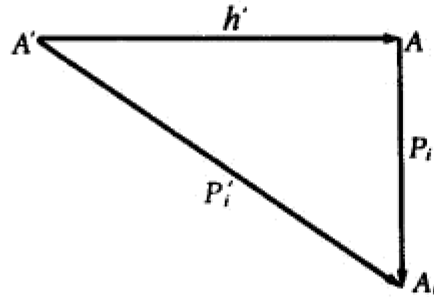
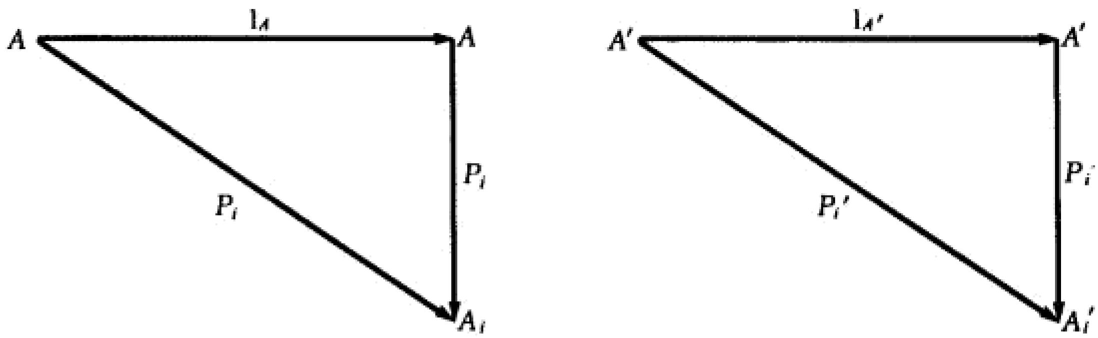


图 5-29



(a) (b)

图 5-30

因此 h 是同构,且 $h' = h^{-1}$。

由此命题,可将 $\mathscr{C}$ 中任意两个对象 A_1, A_2 的积记做

$$A_1 \prod A_2$$

定义 5.5.1 可以推广到任意多个对象的积。

定义 5.5.2 设 $\mathscr{C}$ 是一个范畴, $\forall A_\alpha \in \mathrm{ob}\,\mathscr{C}, \alpha \in I$($I$ 为任一标集),称 $\prod A_\alpha$ 为 A_α 的积,如果对 $\{A_\alpha, P_\alpha \mid \alpha \in I, P_\alpha \in \mathrm{hom}_{\mathscr{C}}(\prod A_\alpha, A_\alpha)\}$, $B \in \mathrm{ob}\,\mathscr{C}, f_\alpha \in \mathrm{hom}_{\mathscr{C}}(B, A_\alpha), \alpha \in I$,存在惟一的 $f \in \mathrm{hom}_{\mathscr{C}}(B, \prod A_\alpha)$,使得下面的图形(图 5-31)是可换的。

类似命题 5.5.1,同样可以证明这样定义的积是惟一的。

请看积的几个例子。

例 1 在集范畴 **Set** 中, $A_\alpha \in \mathrm{ob}\,\mathbf{Set}, \alpha \in I$,令 $\prod A_\alpha = \{\eta \mid$

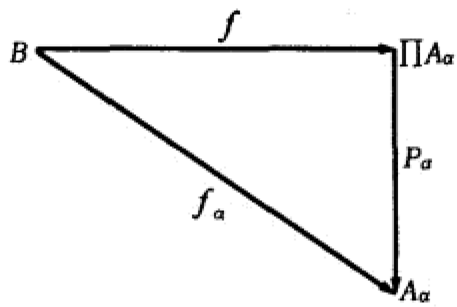


图 5-31

$\eta: I \to \bigcup A_\alpha, \eta(\alpha) \in A_\alpha, \forall \alpha \in I\}$，对 $\forall \alpha \in I$，再令

$$P_\alpha: \prod A_\alpha \to A_\alpha$$
$$\eta \to \eta(\alpha)$$

$\forall B \in \mathrm{ob}\,\mathbf{Set}$，令

$$f_\alpha: B \to A_\alpha$$
$$\zeta \to f_\alpha(\zeta)$$

则存在惟一的

$$f: B \to \prod A_\alpha$$
$$\zeta \to f(\zeta): \alpha \to f_\alpha(\zeta)$$

显然 $P_\alpha f = f_\alpha$，故 $\{\prod A_\alpha, P_\alpha \mid \alpha \in I\}$ 是 A_α 的积。

例 2 在群范畴 **Grp** 中，$G_\alpha \in \mathrm{ob}\,\mathbf{Grp}, \alpha \in I$，令 $G = \prod_{\alpha \in I} G_\alpha$，并定义 $gg'(\alpha) = g(\alpha)g'(\alpha), \forall g, g' \in G; 1(\alpha) = 1_\alpha, 1_\alpha \in G_\alpha$，可以证明 $\{G, P_\alpha\}$ 是 G_α 的积。

例 3 在环范畴 **Ring** 中，$\forall R_\alpha \in \mathrm{ob}\,\mathbf{Ring}$，$\{\prod R_\alpha, P_\alpha\}$ 是 R_α 的积。

关于积的一个对偶概念是上积(coproduct)。

定义 5.5.3 设 $\mathscr{C}$ 是一个范畴，$A_\alpha \in \mathrm{ob}\,\mathscr{C}, \alpha \in I$，称 $\coprod A_\alpha$ 为 A_α 的上积，是指 $\{A, i_\alpha \mid \alpha \in I\}$，其中，$A \in \mathrm{ob}\,\mathscr{C}, i_\alpha \in \hom(A_\alpha, A)$，使得如果 $\forall B \in \mathrm{ob}\,\mathscr{C}, g_\alpha \in \hom(A_\alpha, B)$，均存在惟一的态射

$g \in \hom(A,B)$,使得下面的三角形(图 5-32)可换。

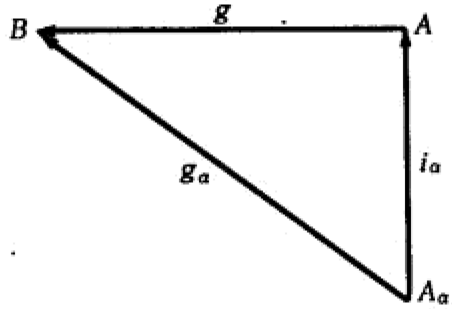


图 5-32

显然,若$\{A, i_\alpha \mid \alpha \in I\}$与$\{A', i_\alpha' \mid \alpha \in I\}$是$A_\alpha$的上积,则存在惟一的同构$k: A' \to A$,使得$i_\alpha = k i_\alpha'$,$\forall \alpha \in I$。在这个意义下,说明上积是惟一的。

例 4 在集范畴 **Set** 中,$A_\alpha \in \text{ob}\,\mathbf{Set}$,$\alpha \in I$,设$\cup A_\alpha$表示$A_\alpha$的不交并,令

$$i_\alpha : A_\alpha \to \cup A_\alpha$$

是单射,设$B \in \text{ob}\,\mathbf{Set}$,并设

$$g_\alpha : A_\alpha \to B$$

则$\exists !\, g: \cup A_\alpha \to B$,使得$g|_{A_\alpha} = g_\alpha$,$\alpha \in I$,故$\{\cup A_\alpha, i_\alpha \mid \alpha \in I\}$是$A_\alpha$的上积。

例 5 在 **R-Mod** 中,再令$M_\alpha \in \text{ob}\,\mathbf{R\text{-}Mod}$,$\alpha \in I$,令$\prod\limits_{\alpha \in I} M_\alpha$是通常的积集合,并具有左 R- 模结构,即$x, y \in \prod M_\alpha$,$r \in R$,并有

$$(x+y)(\alpha) = x(\alpha) + y(\alpha), (rx)(\alpha) = r(x(\alpha))$$

令$\oplus M_\alpha = \{x \mid x(\alpha) = 0$,几乎所有$\alpha \in I\}$,显然$\oplus M_\alpha$是$\prod M_\alpha$的子模。令$x_\alpha \in M_\alpha$,对$\forall \alpha, \beta \in I$,定义

$$i_\alpha x_\alpha(\beta) = \begin{cases} \alpha, \text{当 } \alpha = \beta \text{ 时} \\ 0, \text{当 } \alpha \neq \beta \text{ 时} \end{cases}$$

则 $i_\alpha x_\alpha \bigoplus\limits_{\alpha\in I} M_\alpha$，故

$$i_\alpha : M_\alpha \to \bigoplus M_\alpha$$
$$x_\alpha \to i_\alpha x_\alpha$$

是模同态。

现令 $N \in \text{ob}\ \mathbf{R\text{-}Mod}$，并设 $\forall \alpha \in I, g_\alpha \in \hom_{\mathbf{R\text{-}Mod}}(M_\alpha, N)$，令 $x \in \bigoplus M_\alpha$，则对几乎所有的 $\alpha, x(\alpha) = 0$，因此，$\sum g_\alpha x(\alpha)$ 完全确定，令

$$g : \bigoplus M_\alpha \to N$$
$$x \to \sum g_\alpha x(\alpha)$$

则容易验证 $g \in \hom_{\mathbf{R\text{-}Mod}}(\bigoplus M_\alpha, N)$，且是使 $gi_\alpha = g_\alpha$ 惟一的 g，故 $\{\bigoplus M_\alpha, i_\alpha\}$ 是 M_α 的上积，称为 M_α 的直和。

习题 5.5

1. 设 S 是一个偏序集，**S** 视为范畴(像在 §5.1 例 8 中一样被定义)，设 $\{a_\alpha \mid \alpha \in I\}$ 是 S 中带有下标的元素的集合，给出一个关于 $\{a_\alpha\}$ 的条件，使得在 S 中对应的对象集合有积(上积)，用这个来构造一个范畴，使对象的每个有限子集有积(上积)，但却存在对象的无限集合没有积(上积)。
2. 一个范畴 $\mathscr{C}$ 被称为具有积(上积)的范畴是指在 $\mathscr{C}$ 中任何一对对象在 $\mathscr{C}$ 中有积(上积)。证明：如果 $\mathscr{C}$ 是具有积(上积)的范畴，则在 $\mathscr{C}$ 中对象的任何有限集合有积(上积)。
3. 一个范畴 $\mathscr{C}$ 的对象 A 被称为始对象(终对象)是指 $\mathscr{C}$ 的每个对象 X，$\hom_{\mathscr{C}}(A, X)$($\hom_{\mathscr{C}}(X, A)$) 是一个单元集；一个对象既是始对象又是终对象被称为 $\mathscr{C}$ 的一个零对象。证明：如果 A, A' 是始对象(终对象)，则在 $\hom_{\mathscr{C}}(A, A')$ 中，存在惟一的同构。

4. 设 $A_1, A_2 \in \text{ob}\,\mathscr{C}$，并令 $\mathscr{C}/\{A_1, A_2\}$ 是在习题 5.1 第 4 题中所定义的范畴，证明：在 $\mathscr{C}$ 中，A_1, A_2 有积的充要条件是 $\mathscr{C}/\{A_1, A_2\}$ 有一个终对象，这表明本题和上面的第 3 题一起给出了命题 5.5.1 的另一种证明，并将这个结论推广到 $\mathscr{C}$ 中任意多个对象的集合。

5. 在范畴 $\mathscr{C}$ 中，令 $f_i: A_i \to B$，$i = 1,2$，定义 $\{f_1, f_2\}$ 的拉回图（图 5-33）是一个可换矩形，使得对任意一个包含 f_1 和 f_2 的可换

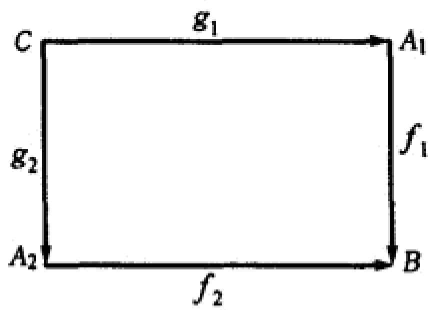


图 5-33

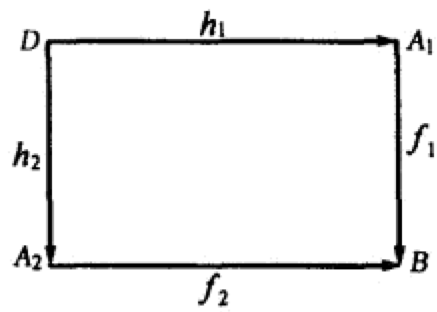


图 5-34

矩形（图 5-34），都存在一个惟一的 $k: D \to C$，使下图（图 5-35）可换。证明：如果 (C, g_1, g_2) 和 (C', g_1', g_2') 确定了 f_1 和 f_2 的拉回图，则存在一个惟一的同构 $k: C' \to C$，使得 $g_i' = g_i k$，$i = 1,2$。

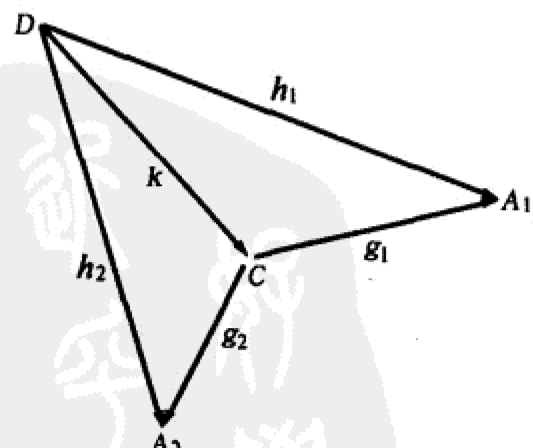


图 5-35

6. 设在范畴 **Grp** 中，$f_i: G_i \to H$，设 M 是 $G_1 \times G_2$ 中满足 $f_1(a_1)$

$=f_2(a_2)$的元素(a_1,a_2)的集合，显然这是一个子群，设$m_i=P_i\mid_M$，其中P_i是$G_1\times G_2$到G_i的投影。证明：(m_1,m_2)定义了一个f_1和f_2的拉回图。

§5.6 hom 函子与可表函子

本节讨论由一个已知的范畴$\mathscr{C}$，以及它的对偶范畴$\mathscr{C}^{OP}$和积范畴$\mathscr{C}^{OP}\times\mathscr{C}$到集范畴**Set**的函子。我们首先研究由$\mathscr{C}^{OP}\times\mathscr{C}$到**Set**的函子。

由积范畴的定义（定义5.1.6），若$A,B\in \mathrm{ob}\,\mathscr{C}$，则$(A,B)\in \mathrm{ob}\,(\mathscr{C}^{OP}\times\mathscr{C})$，且$(f,g)\in \hom_{\mathscr{C}^{OP}\times\mathscr{C}}((A,B),(A',B'))$，此处

$$f\in \hom_{\mathscr{C}^{OP}}(A',A),\ g\in \hom_{\mathscr{C}}(B,B')$$

且若

$$(f',g')\in \hom_{\mathscr{C}^{OP}\times\mathscr{C}}((A',B'),(A'',B''))$$

则

$$f'\in \hom_{\mathscr{C}^{OP}}(A'',A'),\ g'\in \hom_{\mathscr{C}}(B',B'')$$

因而

$$(f',g')(f,g)=(ff',g'g)$$
$$1_{(A,B)}=(1_A,1_B)$$

定义5.6.1 从$\mathscr{C}^{OP}\times\mathscr{C}$到集范畴**Set**的一个函子hom称为hom函子，如果它满足：

(1) $\forall (A,B)\in \mathrm{ob}(\mathscr{C}^{OP}\times\mathscr{C})$，均有$\hom(A,B)\in \mathrm{ob}\,\mathbf{Set}$；

(2) $\forall (f,g)\in \hom_{\mathscr{C}^{OP}\times\mathscr{C}}((A,B),(A',B'))$，均有$\hom(f,g)\in \hom_{\mathscr{C}}(\hom(A,B),\hom(A',B'))$。

其中，$\hom(f,g)(k)\triangleq gkf$，$f\in \hom_{\mathscr{C}^{OP}}(A',A)$，$g\in \hom_{\mathscr{C}}(B,B')$，$k\in \hom_{\mathscr{C}}(A,B)$，故$gkf\in \hom_{\mathscr{C}}(A',B')$。

下面我们指出，这样定义的hom函子是合理的。

命题 5.6.1　hom 函子满足函子定义中的两个条件：

(1)$\hom((f',g')(f,g)) = \hom(f',g')\cdot\hom(f,g)$；

(2)$\hom(1_A,1_B) = 1_{\hom(A,B)}$。

证　(1) $\hom((f',g')(f,g))(k) =$

$$\hom(ff',g'g)(k) =$$
$$(g'g)k(ff') =$$
$$g'\hom(f,g)(k)f' =$$
$$\hom(f',g')\cdot(\hom(f,g)(k))$$

故 $\hom((f',g')(f,g)) = \hom(f',g')\cdot\hom(f,g)$。

(2) 因 $\hom(f,g)(k) \triangleq gkf$，令 $f = 1_A, g = 1_B$，则

$$\hom(1_A,1_B)(k) = k, \forall k \in \hom(A,B)$$

故

$$\hom(1_A,1_B) = 1_{\hom(A,B)}$$

以下的两个定义是 hom 函子的两个特例。

定义 5.6.2　取定 $A \in \mathrm{ob}\,\mathscr{C}$，如果对 $\forall B,B' \in \mathrm{ob}\,\mathscr{C}$，$\forall g \in \hom(B,B')$，规定

$$\hom(A,-)(B) = \hom(A,B)$$
$$\hom(A,-)(g) \triangleq \hom(A,g)$$

其中

$$\hom(A,g):\hom(A,B)\to\hom(A,B')$$
$$k \to gk$$

则称 $\hom(A,-)$ 为由 A 决定的 hom 函子。

定义 5.6.3　取定 $B \in \mathrm{ob}\,\mathscr{C}$，如果对 $\forall A,A' \in \mathrm{ob}\,\mathscr{C}$，$\forall f \in \hom(A',A)$，规定

$$\hom(-,B)A \triangleq \hom(A,B)$$

$$\hom(-,B)(f) \triangleq \hom(f,B) \in \hom(\hom(A,B),\hom(A',B))$$

其中 $\hom(f,B)(k) \triangleq kf$，$\forall k \in \hom(A,B)$，则称 $\hom(-,B)$ 为由 B 决定的反变函子。

设 $f \in \hom(A',B)$，$g \in \hom(B,B')$，$k \in \hom(A,B)$，则由上面的两个定义可得

$$\hom(f,B')\hom(A,g)(k) = (gk)f$$

$$\hom(A',g)\hom(f,B)(k) = g(kf)$$

而 $(gk)f = g(kf) = \hom(f,g)(k)$，故得下面的矩形(图 5-36)是可换的。

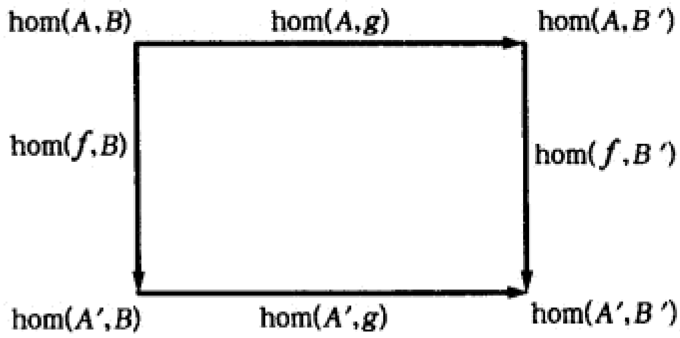


图 5-36

由这个矩形可换，可得两个自然变换。

其一，取定 $g \in \hom(B,B')$，从反变函子 $\hom(-,B)$ 到反变函子 $\hom(-,B')$ 的自然变换 $\eta \triangleq \hom(-,g)$，$\eta_A = \hom(A,g)$，$\eta_{A'} = \hom(A',g)$，因对 $\forall A \in \mathrm{ob}\,\mathscr{C}$，有

$$\eta_A = \hom(A,g) \in \hom_{\mathbf{Set}}(\hom(A,B),\hom(A,B'))$$

且由图形可换，可知 η 是一个自然变换。

其二，同理 $\eta' \triangleq \hom(f,-)$，$\eta'_B = \hom(f,B)$，则 η' 是由共变函子 $\hom(A,-)$ 到共变函子 $(A',-)$ 的一个自然变换。

hom 函子是一个很具体的函子，它可以计算出来。那么可否将任意一个抽象函子 F 都由 hom 函子表示出来？为此需证一个较深的引理。

Yoneda 引理 设 F 是由 $\mathscr{C}$ 到 **Set** 的一个函子，$A \in \mathrm{ob}\,\mathscr{C}$，$a \in FA$，令

$$a_B : \hom(A,B) \to FB$$

$$k \to F(k)a$$

则

(1) $B \xrightarrow{\eta(a)} a_B$ 是函子 $\hom(A,-)$ 到函子 F 的自然变换；

(2) $a \to \eta(a)$ 是集合 FA 与 $\hom(A,-)$ 到 F 的自然变换类的双射，其逆为 $\eta \to \eta_A(1_A) \in FA$。

证 (1) 令 $k \in \hom_{\mathscr{C}}(A,B)$，则 $F(k) \in \hom_{\mathrm{Set}}(FA,FB)$，且 $F(k)(a) \in FB$，故有映射

$$a_B : \hom_{\mathscr{C}}(A,B) \to FB$$
$$k \to F(k)(a)$$

$\forall C \in \mathrm{ob}\,\mathscr{C}$，令 $g \in \hom_{\mathscr{C}}(B,C)$，有

$$F(g)a_B(k) = F(g)F(k)(a) = F(gk)(a)$$
$$a_C\hom(A,g)(k) = a_C(gk) = F(gk)(a)$$

故有下面的矩形(图 5-37)是可换的。

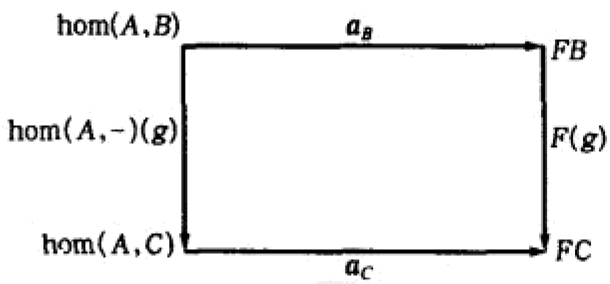


图 5-37

因此，$B \xrightarrow{\eta(a)} a_B$ 是由 $\hom(A,-)$ 到 F 的自然变换，且 $(\eta(a))_A(1_A) = a_A(1_A) = F(1_A)(a) = a$。

(2) 令 η 是由 $\hom(A,-)$ 到 F 的任一自然变换，设 $f \in \hom_{\mathscr{C}}(A,B)$，则由下面图形(图 5-38)的可换性可以推出

$$\eta_B(f) = \eta_B(f1_A) = \eta_B(\hom(A,f)(1_A)) \xlongequal{\text{可换性}}$$
$$F(f)\eta_A(1_A) = F(f)(a)$$

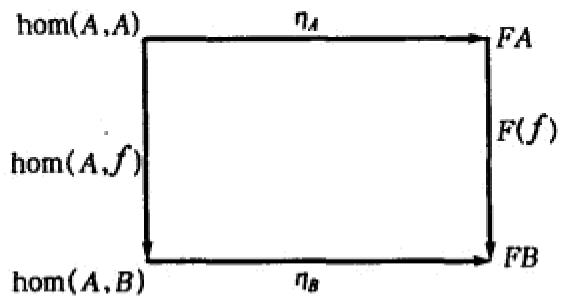


图 5-38

故 $\eta = \eta(a)$。

定义 5.6.4 称由$\mathscr{C}$到**Set**的函子 F 为可表函子，如果对 $A \in \mathrm{ob}\,\mathscr{C}$，存在 F 到 $\hom(A, -)$ 的自然同构。

如果 η 是这个自然同构，η 由 A 决定，a 由 η_A 决定，则 $a = \eta_A(1_A)$，因而由 Yoneda 引理和定义 5.6.4 可得下面的定理。

定理 5.6.1 （表示定理）

任一函子均可用 hom 函子表示出来。称(A, a)为可表函子 F 的一个表示。

习题 5.6

1. 应用 Yoneda 引理来获得集合 $\hom_{\mathscr{C}}(A, B)$ 上的 $\hom(A, -)$ 到 $\hom(A', -)$ 的自然变换类的双射。
2. 证明：在范畴$\mathscr{C}$中，$f: B \to B'$ 是单态射当且仅当对$\mathscr{C}$中的每一个对象 A，$\hom(A, f)$ 是单射。
3. 如果 F 是从$\mathscr{C}$到**Set**的逆变函子，$A \in \mathrm{ob}\,\mathscr{C}$，则 $\hom_{\mathscr{C}}(-, A)$ 到 F 的任一自然变换都是$B \to a_B$，其中 a_B 是 $\hom_{\mathscr{C}}(B, A)$ 到 FB 的一个映射；FB 由$a_B: k \to F(k)a$ 所确定，其中 $a \in FA$。运用 Yoneda 引理的对偶命题来证明：用这种方式得到从 $\hom_{\mathscr{C}}(-, A)$ 到 F 的自然变换类的集合 FA 的一个双射。

第6章　*CF* 范畴

本章是在上一章的基础上，将经典的范畴(Classical Category)和近年来发展起来的模糊范畴(Fuzzy Category)融为一体，阐述了 *CF* 范畴的一些基本概念。这种 *CF* 范畴起着通观的作用，广泛应用于量子场论和 DNA 分子生物等领域的研究中，是一个颇有发展前景的新兴领域。

§6.1　*CF* 集范畴

范畴的模糊化[①] 工作包括两个方面：一是对象的模糊化，二是态射的模糊化。将对象模糊化，自然引进模糊集合的范畴 **Set(L)** 的概念。为此，先介绍模糊函数的概念。

定义 6.1.1　设 X 和 Y 是两个论域，A 和 B 分别是 X 和 Y 的模糊子集，令

$$f: X \to Y$$

f 称为具有模糊定义域和模糊值域的模糊函数当且仅当 $\forall x \in X, B(f(x)) \geqslant A(x)$，记做 $f: A \to B$。

例1　好工人得到高工资。

令 $X = \{某工厂工人\}, Y = (0, +\infty)$。

设 A 是好工人的模糊子集，B 是高工资的模糊子集，令

$$f: X \to Y$$

即工厂的每一个工人都对应一份工资，而

---

① 汪培庄．模糊集与模糊集范畴．数学进展，1982(1)：1～8

$$B(f(x)) \geqslant A(x)$$

就是好工人得到高工资的描述。

例 2 大卡车必须慢走。

令 $X = \{卡车\}, Y = \{速度\}$, A 表示大卡车, B 表示低速度, 则

$$B(f(x)) \geqslant A(x)$$

意味着卡车越大,它的速度应越慢。

日常生活中的许多话都可以用模糊函数来描述。例如“酒饮得越少,气血越平和,头脑越清醒”、“工作越努力,成绩越大” 等等。

现在给出 CF 集范畴的定义。

定义 6.1.2 令 L 是完全格,称 **Set(L)** 为 CF 集范畴,如果 **Set(L)** 的对象是 L 模糊集,即 (X, A),其中 X 是论域, A 是 X 到 L 的一个映射, **Set(L)** 的态射是模糊函数 $f: A \to B$,即图 6-1,满足 $B(f(x)) \geqslant A(x) \quad (\forall x \in X)$。

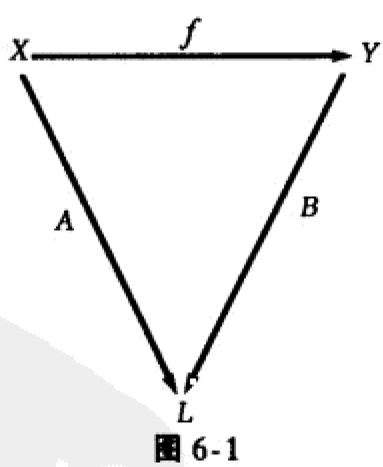


图 6-1

显然 **Set(L)** 是满足范畴定义的,只需注意到下面的事实:

$\forall f \in \hom((X, A), (Y, B)), \forall g \in \hom((Y, B), (Z, C))$,有

$$C((g \circ f)(x)) \geqslant B(f(x)) \geqslant A(x) \quad (\forall x \in X)$$

则

$$g \circ f \in \hom((X, A), (Z, C))$$

容易验证。满足态射合成运算的几个条件。

例 3 设 $L=[0,1]$, $X=\{x_1,x_2,x_3\}$, $Y=\{y_1,y_2,y_3\}$,

$$A=\frac{0.2}{x_1}+\frac{0.4}{x_2}+\frac{0.6}{x_3}$$

$$B=\frac{0.3}{y_1}+\frac{0.5}{y_2}+\frac{0.7}{y_3}$$

故 (X,A), (Y,B) 为 **Set(L)** 的对象,态射是模糊函数 f_1, f_2, f_3 等(参看图 6-2)。

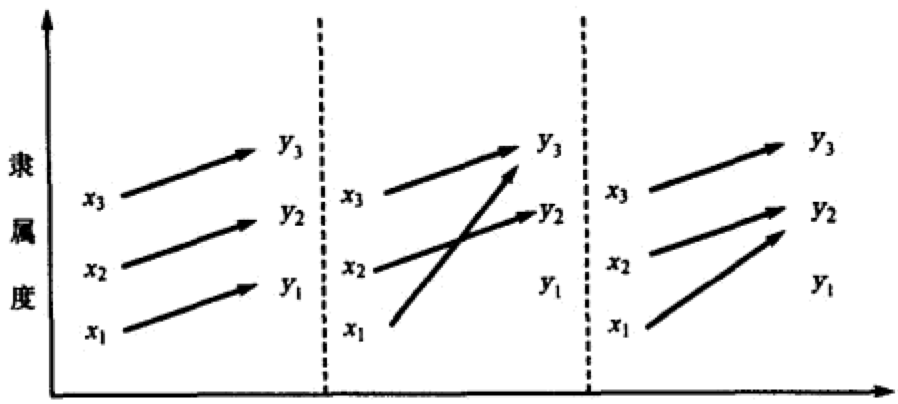


图 6-2

由图 6-2 看出 $B(f_i(x_j)) \geqslant A(x_j)$, $i,j=1,2,3$。

定义 6.1.3 设范畴的对象是 (X,A), $A:X\to L$,态射是模糊关系 R,且满足

$$R(x,y)\leqslant A(x)\wedge B(y)\quad(\forall x\in X,\forall y\in Y)$$

这个范畴叫 **Set$_f$(L)**。

只需注意到,若 $R\in \hom((X,A),(Y,B))$ 有

$$R(x,y)\leqslant A(x)\wedge B(y)$$

若 $S\in \hom((Y,B),(Z,C))$ 有

$$S(y,z)\leqslant B(y)\wedge C(z)$$

则

$$R\circ S(x,z)=\bigvee_{y\in Y}(R(x,y)\wedge S(y,z))\leqslant$$

$$\bigvee_{y\in Y}(A(x)\wedge B(y)\wedge B(y)\wedge C(z))\leqslant$$

$$A(x)\wedge C(z)$$

$\mathbf{Set}_f(\mathbf{L})$ 的定义就是合理的。

定义 6.1.4 设范畴的对象是(X,A)，$A:X\to L$，其态射为满足

$$\bigvee_{x\in X}(R(x,y)\wedge A(x))\leqslant B(y)\quad(\forall y\in Y)$$

的模糊关系 R，这个范畴叫做 $\mathbf{Set}_g(\mathbf{L})$。

这个定义也是合理的，因由模糊关系的合成，显然有

$$\bigvee_{x\in X}(R\circ S(x,z)\wedge A(x))=$$

$$\bigvee_{x\in X}((\bigvee_{y\in Y}(R(x,y)\wedge S(y,z)))\wedge A(x))=$$

$$\bigvee_{y\in Y}\bigvee_{x\in X}(R(x,y)\wedge S(y,z)\wedge A(x))\leqslant$$

$$\bigvee_{y\in Y}(S(y,z)\wedge B(y))\leqslant C(z)$$

例 4 设 $L=[0,1]$，$X=\{x_1,x_2,x_3\}$，$Y=\{y_1,y_2\}$，

$$A=\frac{0.5}{x_1}+\frac{0.7}{x_2}+\frac{0.2}{x_3},B=\frac{0.8}{y_1}+\frac{0.6}{y_2}$$

R 的模糊关系矩阵为

$$\begin{array}{cc} & \begin{array}{cc} y_1 & y_2 \end{array} \\ \boldsymbol{R}= & \begin{bmatrix} 0.4 & 0.5 \\ 0.6 & 0.6 \\ 0.1 & 0.2 \end{bmatrix} \begin{array}{c} x_1 \\ x_2 \\ x_3 \end{array} \end{array}$$

容易验证 $R(x_i,y_j)\leqslant A(x_i)\wedge B(y_j)$，$i=1,2,3$，$j=1,2$，故 $\boldsymbol{R}$ 是 $\mathbf{Set}_f(\mathbf{L})$ 的态射。又

$$\bigvee_{i=1}^{3}(R(x_i,y_1)\wedge A(x_i))=$$

$$(0.4\wedge 0.5)\vee(0.6\wedge 0.7)\vee(0.1\wedge 0.2)=$$

$$0.4\vee 0.6\vee 0.1=0.6\leqslant 0.8=B(y_1)$$

$$\bigvee_{i=1}^{3}(R(x_i,y_2)\wedge A(x_i))=$$
$$(0.5\wedge 0.5)\vee(0.6\wedge 0.7)\vee(0.2\wedge 0.2)=$$
$$0.5\vee 0.6\vee 0.2=0.6\leqslant 0.6=B(y_2)$$

故 R 也是 $\mathbf{Set}_g(\mathbf{L})$ 的映射。

从以上定义可以看出，范畴是一个数学结构的外延，其内涵由态射来保持，态射下的不变性质就是这个数学结构的性质。

现在我们来讨论这几个范畴之间的关系，先构造一个从 $\mathbf{Set}(\mathbf{L})$ 到 $\mathbf{Set}_f(\mathbf{L})$ 的函子 F：

(1) $$F:\mathrm{ob}\ \mathbf{Set}(\mathbf{L})\to \mathrm{ob}\ \mathbf{Set}_f(\mathbf{L})$$
$$(X,A)\to(X,A)$$

(2) $\forall f\in \mathrm{hom}((X,A),(Y,B))$，令 $F(f)=R_f$，

$$R_f(x,y)=\begin{cases}A(x), & \text{当 } f(x)=y \text{ 时}\\ 0, & \text{当 } f(x)\neq y \text{ 时}\end{cases}$$

易见，当 $f(x)=y$ 时，有

$$R_f(x,y)=A(x)\leqslant B(f(x))=B(y)$$

从而 $R_f(x,y)\leqslant A(x)\wedge B(y)$。

当 $f(x)\neq y$ 时，$R_f(x,y)=0$，上式依然成立，故

$$F(f)\in \mathrm{hom}(F(X,A),F(Y,B))$$

显然有

$$F(g\circ f)=R_{g\circ f}=R_g\circ R_f=F(g)\circ F(f)$$
$$F(1_A)=R_{1_A}=1_{F(A)}$$

故

$$F:\mathbf{Set}(\mathbf{L})\to \mathbf{Set}_f(\mathbf{L})$$

是一个函子，但这个函子不能使两个范畴同构。

又在 $\mathbf{Set}_f(\mathbf{L})$ 与 $\mathbf{Set}_g(\mathbf{L})$ 之间构造一个函子 G：

(1) $$G:\mathrm{ob}\ \mathbf{Set}_f(\mathbf{L})\to \mathrm{ob}\ \mathbf{Set}_g(\mathbf{L})$$

$$(X,A) \to (X,A)$$

(2) $\forall R \in \hom((X,A),(Y,B))$，令 $G(R) = R$，因为

$$R(x,y) \leqslant A(x) \wedge B(y)$$

则有

$$R(x,y) \wedge A(x) = R(x,y)$$

故 $\bigvee_{x \in X}(R(x,y) \wedge A(x)) = \bigvee_{x \in X} R(x,y) \leqslant \bigvee_{x \in X} B(y) = B(y)$，因此 R 也是 ob $\mathbf{Set}_g(\mathbf{L})$ 中的态射。

由以下结果，下图(图 6-3)中从 $\mathbf{Set}(\mathbf{L})$ 到 $\mathbf{Set}_g(\mathbf{L})$ 的函子可以作为 $F \circ G$ 来考察。

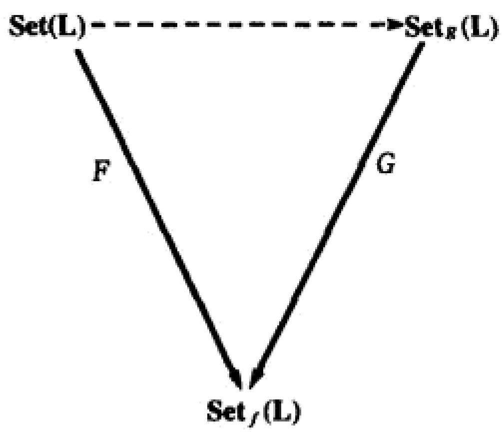


图 6-3

一旦范畴 $\mathbf{Set}(\mathbf{L})$ 被给出，就可以分别构成 $\mathbf{Set}_f(\mathbf{L})$ 和 $\mathbf{Set}_g(\mathbf{L})$。在此意义下，$\mathbf{Set}(\mathbf{L})$ 是基本的，它有着颇有兴趣的直观背景，将其性质叙述如下：

$\mathbf{Set}(\mathbf{L})$ 的态射是模糊函数，由模糊函数的定义，$\forall \alpha \in L$，有

$$A_\alpha \leqslant (B \circ f)_\alpha$$

这意味着，若 x 在 α 的水平上属于 A，则 $f(x)$ 在 α 的水平上必属于 B，这正是经典映射的推广。

将态射模糊化是模糊范畴理论的另一方面的工作，这个工作应归于 Goguen。

定义 6.1.5 设 $\mathscr{L}$ 为一个范畴，称 $\mathscr{L}_L$ 为 $\mathscr{L}$ 的(态射)的模糊化范畴，如果：

(1) $\mathrm{ob}\,\mathscr{L}_L = \mathrm{ob}\,\mathscr{L}$；

(2) $\forall A, B \in \mathrm{ob}\,\mathscr{L}$，定义

$$\hom^*(A,B) = \mathscr{F}_L(\hom^*(A,B)) = \{S \mid S:\hom^*(A,B) \to L\}$$

作为 $\mathscr{L}_L$ 的模糊态射集。

模糊态射的合成运算定义为：

$\forall S \in \hom^*(A,B), T \in \hom^*(B,C)$，定义 $T\Delta S \in \hom^*(A,C)$：$T\Delta S(h) = \bigvee_{g\cdot f=h}(S(f) \wedge T(g))$，$\forall h \in \hom(A,C)$，此处 $f \in \hom(A,B)$，$g \in \hom(B,C)$，$g \circ f$ 是 $\mathscr{L}$ 中态射的合成运算，当 $\{(g,f) \mid g \circ f = h\} = \varnothing$ 时，空指标集取上确界规定为 0(L 中的最小元)，并称 $1_A \in \hom^*(A,A)$ 为模糊恒等态射，如果

$$1_A(f) = \begin{cases} 1, f = 1_A \\ 0, f \neq 1_A, f \in \hom(A,A) \end{cases}$$

为验证定义的合理性，我们有如下的定理。

定理 6.1.1 设 $\mathscr{L}$ 为范畴，则 $\mathscr{L}_L$ 必为范畴。

证 $\mathscr{L}$ 的对象集与 $\mathscr{L}_L$ 的对象集相同，且 $\forall A, B \in \mathscr{L}_L$，有一个从 A 到 B 的模糊态射集 $\hom^*(A,B)$，模糊态射的合成运算 Δ 也给出，关键是验证。

(1) Δ 满足结合律。

$\forall T \in \hom^*(A,B), S \in \hom^*(B,C), R \in \hom^*(C,D)$，设 $f \in \hom(A,B)$，$g \in \hom(B,C)$，$h \in \hom(C,D)$，$p \in \hom(D,A)$，则

$$R\Delta(S\Delta T)(p) = \bigvee_{h\cdot q=p}(R(h) \wedge S\Delta T(q)) =$$

$$\bigvee_{p=h\cdot q}(R(h)) \wedge \bigvee_{q=g\cdot f}(S(g) \wedge T(f)) =$$

$$\bigvee_{p=h\cdot q}\bigvee_{q=g\cdot f}(R(h) \wedge S(g) \wedge T(f)) =$$

$$\bigvee_{p=h\cdot(g\cdot f)}(R(h) \wedge S(g) \wedge T(f)) =$$

$$\bigvee_{p=(h\cdot g)\cdot f}(R(h) \wedge S(g) \wedge T(f)) =$$

$$\bigvee_{p=q\cdot f}\bigvee_{q=h\cdot g}(R(h) \wedge S(g) \wedge T(f)) =$$

$$\bigvee_{p=q\cdot f}((\bigvee_{q=h\cdot g}(R(h) \wedge S(g))) \wedge T(f)) =$$

$$\bigvee_{p=q\cdot f}(R\Delta S(q) \wedge T(f)) =$$

$$(R\Delta S)\Delta T(p)$$

上述各等式对取上确界之指标集为空集时,显然成立,故

$$R\Delta(S\Delta T) = (R\Delta S)\Delta T$$

(2) $\forall A \in \text{ob}\,\mathscr{L}_L$,总有 $1_A \in \text{hom}^*(A,A)$,满足

$$1_A\Delta S = S \quad (S \in \text{hom}^*(B,A), B \in \text{ob}\,\mathscr{L}_L)$$

$$T\Delta 1_A = T \quad (T \in \text{hom}^*(A,B), B \in \text{ob}\,\mathscr{L}_L)$$

事实上,取

$g \in \text{hom}(B,A), f \in \text{hom}(A,A), f' \in \text{hom}(B,A)$,有

$$1_A\Delta S(g) = \bigvee_{g=f\cdot f'}(1_A(f) \wedge S(f')) =$$

$$\bigvee_{g=1_A\cdot f'}S(f') = S(g) \quad (f = 1_A)$$

故 $1_A\Delta S = S$,同理可证 $T\Delta 1_A = A$。

(3) 若 $(A,B) \neq (A',B')$,则

$$\text{hom}(A,B) \cap \text{hom}(A',B') = \varnothing$$

而 $\quad \text{hom}^*(A,B) = \{S \mid S:\text{hom}(A,B) \to L\}$

$\quad \text{hom}^*(A',B') = \{T \mid T:\text{hom}(A',B') \to L\}$

显然有

$$\text{hom}^*(A,B) \cap \text{hom}^*(A',B') = \varnothing$$

最后指出，汪培庄教授利用 L 集论和模糊场的概念引进了两个新的范畴 $U(L)$ 和 $\sum(L)$，并证明了它们皆与 Set(L) 同构。他还运用范畴理论，重新解释了扩展原理的合理性。刘应明教授通过一个对象对应一组单位元引入了准范畴的概念。1971 年，Poston 还定义了称为“Fuz”的范畴，其对象是附有非模糊的近似关系的集合。Dodson 于 1974 年推广了他的工作，提出“hazy”空间，他指出，在“Fuz”和“hazy”空间的情况下与实际经验类似，可以用有限的精度测量，Dodson 还用例子说明，用“hazy”空间去模拟基本质点将是一个好的工具，这里不做介绍。

§6.2 CF 群范畴

在本节中，L, L_1, L_2 都表示有最大元 1 和最小元 0 的完全分配格，其格运算都记为 $\wedge$，$\vee$，格的半序记为 $\leqslant$，X, X_1, X_2 都表示群。

设 X 是群，$A: X \to L$，若对 $\forall x, y \in X$，有

$$A(xy) \geqslant A(x) \wedge A(y)$$
$$A(x^{-1}) = A(x)$$

则称 A 为 X 的 LF 子群[①]，X 的所有 LF 子群记为 $F_L(X)$。

设 $\varphi: L_1 \to L_2$，若对 $\forall \{a_i\}_{i\in I} \subset L_1$，有 $\varphi(\bigvee_{i\in I} a_i) = \bigvee_{i\in I} \varphi(a_i)$，则称 φ 为保并运算，对于交运算 $\wedge$ 也有类似的定义。

定义 6.2.1 设 $A \in F_{L_1}(X_1)$，$B \in F_{L_2}(X_2)$，A 到 B 的同态映射是映射对 (f, φ)，满足：

(1) $f: X_1 \to X_2$ 是群同态映射；

(2) $\varphi: L_1 \to L_2$ 是保并和保交运算，且 $\varphi(0) = 0 \in L_2$；

---

① 邹开其．CF 代数．石家庄：河北教育出版社，1993

(3) $A=\varphi^{-1}Bf$，其中 φ^{-1} 定义为

$$\varphi^{-1}(\alpha)=\vee\{\beta\mid\varphi(\beta)\leqslant\alpha,\beta\in L_1\}\quad(\forall\alpha\in L_2)$$

A 到 B 的所有同态映射记为 $\hom(A,B)$。

定理 6.2.1 设 $(f,\varphi)\in\hom(A,B)$，$(g,\psi)\in\hom(B,C)$，规定运算

$$(g,\psi)(f,\varphi)=(gf,\psi\varphi)\tag{a}$$

则 $(g,\psi)(f,\varphi)\in\hom(A,C)$，且这个运算满足结合律。

证 显然有 gf 仍是群同态，$\psi\varphi$ 保持任意并和任意交，下证 $A=(\psi\varphi)^{-1}C(gf)$，为此先证

$$\varphi(\alpha)\leqslant\beta\Leftrightarrow\alpha\leqslant\varphi^{-1}(\beta)$$

$\varphi(\alpha)\leqslant\beta\Rightarrow\alpha\leqslant\varphi^{-1}(\beta)$ 显然成立。

反之，若 $\alpha\leqslant\varphi^{-1}(\beta)$，由 φ 的保并和保交性，有

$$\varphi(\alpha)\leqslant\varphi(\varphi^{-1}(\beta))=\varphi(\vee\{\gamma\mid\varphi(\gamma)\leqslant\beta\})=$$
$$\vee\{\varphi(\gamma)\mid\varphi(\gamma)\leqslant\beta\}\leqslant\beta$$

从而有

$$(\psi\varphi)^{-1}(\alpha)=\vee\{\beta\mid\psi\varphi(\beta)\leqslant\alpha\}=$$
$$\vee\{\beta\mid\varphi(\beta)\leqslant\psi^{-1}(\alpha)\}=$$
$$\varphi^{-1}((\psi^{-1})(\alpha))=\varphi^{-1}\psi^{-1}(\alpha)$$

即 $(\psi\varphi)^{-1}=\varphi^{-1}\psi^{-1}$。故 $A=\varphi^{-1}Bf=\varphi^{-1}\psi^{-1}Cgf=(\psi\varphi)^{-1}C(gf)$。即

$$(g,\psi)(f,\varphi)\in\hom(A,C)$$

结合律显然成立。

下面的两个命题给出了同态映射的基本性质。

命题 6.2.1 设 $B\in F_{L_2}(X_2)$，$A\in L_1{}^{X_1}$，若有映射对 (f,φ) 满足定义 6.2.1 中条件(1)～(3)，则 $A\in F_{L_1}(X_1)$。

证 先证 φ^{-1} 保持任意交。

设 $\{\alpha_t\}_{t\in T}\subseteq L_2$，则

$$\varphi^{-1}(\bigwedge_{t\in T}\alpha_t) = \{\beta \mid \varphi(\beta) \leqslant \bigwedge_{t\in T}\alpha_t, \beta \in L_1\} =$$

$$\bigvee\{\beta \mid \varphi(\beta) \leqslant \alpha_t, \forall t \in T, \beta \in L_1\} =$$

$$\bigvee\{\beta \mid \beta \leqslant \varphi^{-1}(\alpha_t), \forall t \in T, \beta \in L_1\} =$$

$$\bigvee\{\beta \mid \beta \leqslant \bigwedge_{t\in T}\varphi^{-1}(\alpha_t), \beta \in L_1\} =$$

$$\bigwedge_{t\in T}\varphi^{-1}(\alpha_t)$$

从而 φ^{-1} 也保序，由 $A = \varphi^{-1}Bf$，易验证 $A \in F_{L_1}(X_1)$。

命题 6.2.2 设 $A \in F_{L_1}(X_1)$，(f, φ) 满足定义 6.2.1 中的条件(1) 和(2)，$B \in L_2^{X_2}$，定义为

$$B(x) = \bigvee_{x_1 \in f^{-1}(x)} \varphi(A(x_1)), \forall x \in X_2$$

则 $B \in F_{L_2}(X_2)$，且 $\varphi^{-1}Bf \supseteq A$，空集的上确界定义为 0。

证 设 $x, y \in X_2$，若 $B(x)$ 与 $B(y)$ 中至少有一个为 0，则显然有

$$B(xy) \geqslant B(x) \wedge B(y)$$

若 $B(x) \neq 0, B(y) \neq 0$，则

$$f^{-1}(x) \neq \varnothing, f^{-1}(y) \neq \varnothing$$

因而 $f^{-1}(xy) \neq \varnothing$，故

$$B(xy) = \bigvee_{x_1 \in f^{-1}(xy)} \varphi(A(x_1)) =$$

$$\bigvee_{xy = f(x_1)} \varphi(A(x_1)) \geqslant$$

$$\bigvee_{\substack{x = f(x_1') \\ y = f(x_1'')}} \varphi(A(x_1' x_1'')) \geqslant$$

$$\bigvee_{\substack{x = f(x_1') \\ y = f(x_1'')}} \varphi(A(x_1') \wedge A(x_1'')) =$$

$$\bigvee_{\substack{x = f(x_1') \\ y = f(x_1'')}} \varphi(A(x_1')) \wedge \varphi(A(x_1'')) =$$

$$(\bigvee_{x=f(x_1')}\varphi(A(x_1'))) \wedge (\bigvee_{y=f(x_1'')}\varphi(A(x_1''))) =$$

$$B(x) \wedge B(y)$$

$$B(x^{-1}) =$$

$$\bigvee_{x_1\in f^{-1}(x^{-1})}\varphi(A(x_1)) =$$

$$\bigvee_{f(x_1)=x^{-1}}\varphi(A(x_1)) =$$

$$\bigvee_{x=f(x_1^{-1})}\varphi(A(x_1)) =$$

$$\bigvee_{x=f(x_1^{-1})}\varphi(A(x_1^{-1})) =$$

$$\bigvee_{x=f(y_1)}\varphi(A(y_1)) = B(x)$$

即 $B \in F_{L_2}(X_2)$。

$$\varphi^{-1}Bf(x_1) = \varphi^{-1}(B(f(x_1))) =$$

$$\varphi^{-1}(\bigvee_{f(x_1)=f(x)}\varphi(A(x))) \geqslant$$

$$\varphi^{-1}(\varphi(A(x_1))) =$$

$$\vee\{\beta \mid \varphi(\beta) \leqslant$$

$$\varphi(A(x_1)), \beta \in L_1\} \geqslant A(x_1)$$

$$(\forall x_1 \in X_1)$$

即 $\varphi^{-1}Bf \supseteq A$。

定义 6.2.2 称 **FG** 是一个 *CF* 群范畴[①]，它的对象类为 ob **FG** = $\{A \mid A \in F_L(X)\}$，对 $\forall A, B \in$ ob **FG**，A，B 间的态射集规定为定义 6.2.1 中的 hom(A,B)，态射间的合成运算由定理 6.2.1 中的(a) 式规定。

只需注意到定理 6.2.1，就易证此定义的合理性，注意我们的

---

① 彭先图. Fuzzy 群范畴. 模糊数学，1987(1)：61 ~ 67

范畴定义放弃了条件

$$(A,B) \neq (A',B') \Rightarrow \hom(A,B) \cap \hom(A',B') = \varnothing$$

加上此条件后，命题 6.2.2 可强化为以下的定理。

定理 6.2.2 设 $A \in F_{L_1}(X_1)$，(f,φ) 满足定义 6.2.1 中的条件(1) 和(2)，而且 f 与 φ 均是单射，则按(3) 式定义的 $B \in F_{L_2}(X_2)$，且 $\varphi^{-1}Bf = A$。

证 先证 $\varphi^{-1}(\varphi(\alpha)) = \alpha$，注意 $\varphi(\beta) \leqslant \varphi(\alpha)$ 时必有 $\beta \leqslant \alpha$，因 $\varphi(\beta) = \varphi(\beta) \wedge \varphi(\alpha) = \varphi(\beta \wedge \alpha)$，由 φ 是单射，有

$$\beta = \beta \wedge \alpha \leqslant \alpha$$

从而对 $\forall \alpha \in L_1$，有

$$\varphi^{-1}(\varphi(\alpha)) = \bigvee \{\beta \mid \varphi(\beta) \leqslant \varphi(\alpha), \beta \in L_1\} = \bigvee \{\beta \mid \beta \leqslant \alpha, \beta \in L_1\} = \alpha$$

即 $\varphi^{-1}\varphi = 1_{L_1}$（$1_{L_1}$ 是 L_1 的恒等映射）。

又对 $\forall x \in X_1$，有 $f^{-1}(f(x)) = \{x\}$，故

$$\varphi^{-1}Bf(x) = \varphi^{-1}(B(f(x))) = \varphi^{-1}\Big(\bigvee_{x_1 \in f^{-1}(f(x))} \varphi(A(x_1))\Big) = \varphi^{-1}(\varphi(A(x))) = A(x)$$

即 $\varphi^{-1}Bf = A$。

此定理表明，一般说来，$\hom(A,A)$ 不仅仅含有 $(f,1_L)$。对于特殊情况 $L = \{0,1\}$，定理 6.2.3 将给出详细的说明。

定义 6.2.3 **FG(L)**，**FG(X)**，**FG(φ)** 和 **FG₀** 如下定义，其中所有态射都来自 **FG** 中：

(1) **FG(L)** 的对象类 ob **FG(L)** $= \{A \mid A \in F_L(X)$，X 是任意群，L 是一个指定的完全分配格$\}$；

(2) **FG(X)** 的对象类 ob **FG(X)** $= \{A \mid A \in F_L(X)$，L 是任意的完全分配格，X 是一个指定的群$\}$；

(3) $\mathbf{FG}(\varphi)$ 的对象类 ob $\mathbf{FG}(\varphi)$ = ob $\mathbf{FG}(\mathbf{L})$，态射集为 $\hom(A,B) = \{(f,\varphi) \mid \varphi$ 是一个指定的保并、保交运算$\}$；

(4) $\mathbf{FG}_0 = \mathbf{FG}(\{0,1\})$。

显然，以上 4 种均为 *CF* 群范畴。

命题 6.2.3 $\mathbf{FG}(\mathbf{L})$，$\mathbf{FG}(\mathbf{X})$，$\mathbf{FG}(\varphi)$ 都是 $\mathbf{FG}$ 的子范畴，前两个是完满的子范畴，最后一个不是完满的子范畴。

证 由定义 6.2.3，前两个结论显然成立，最后一个结论是下面的定理 6.2.3 的推论。

定理 6.2.3 设 $L = \{0,1\}$，$A \in F_L(X_1)$，$B \in F_L(X_2)$，$\mathbf{FG}(\mathbf{L}) = \mathbf{FG}_0$ 中的态射集 $\hom(A,B)$ 有如下性质：

(1) 当 $A \neq X_1$ 时，$\hom(A,B)$ 或者是空集，或者 $\hom(A,B) = \{(f,\varphi) \mid f$ 是群同态，$\varphi = 1_L$，$A = Bf\}$；

(2) 若存在 $(f,0) \in \hom(A,B)$，则 $A = X_1$。

证 首先看 $\varphi: L \to L$ 的四种可能：1_L；0；$\varphi_1: 0 \to 1, 1 \to 1$ 和 $\varphi_2: 0 \to 1, 1 \to 0$。前两种都满足定义 6.2.1 中条件(2)，第三种不满足 $\varphi(0) = 0$，第四种不保持任意交。所以 $\hom(A,B)$ 中的元只有两种可能：$(f,1_L)$ 和 $(f,0)$。

(1) 若 $A \neq X_1$，$\hom(A,B) \neq \emptyset$，存在 $(f,\varphi) \in \hom(A,B)$，使 $A = \varphi^{-1}Bf$，φ 只有两种可能：$\varphi = 1_L$ 和 $\varphi = 0$，若 $\varphi = 0$，则 $\varphi^{-1} = \varphi_1$，从而

$$A(x) = \varphi^{-1}Bf(x) = \varphi^{-1}(B(f(x))) = 1 \quad (\forall x \in X_1)$$

即 $A = X_1$，此为矛盾，故 $\varphi \neq 0$。所以 $\varphi = 1_L$，$A = 1_L Bf = Bf$。

(2) 因 $0^{-1} = \varphi_1$，故

$$A = 0^{-1}Bf = \varphi_1 Bf = X_1$$

定理 6.2.4 记 $L = \{0,1\}$，普通群范畴 $\mathbf{Grp}$ 和 $\mathbf{FG}_0(1_L)$ 同构。

定理 6.2.5 $\mathbf{FG}(\varphi)$ 不是 $\mathbf{FG}(\mathbf{L})$ 的完满子范畴，从而它也不

是 **FG** 的完满子范畴。

证 只需证明存在 $A,B \in \mathrm{ob}\,\mathbf{FG}(\boldsymbol{\varphi}) = \mathrm{ob}\,\mathbf{FG}(\mathbf{L})$ 和 $\psi \neq \varphi$，但 $(f,\psi) \in \hom(A,B)$ 在 $\mathbf{FG}(\mathbf{L})$ 中成立。

当 $\varphi \neq 1_L$ 时，取 $A = B = X \in F_L(X)$，取 $\psi = 1_L, f = 1_X$，则 $(f,\psi) \in \hom(A,B)$ 在 $\mathbf{FG}(\mathbf{L})$ 中成立，而在 $\mathbf{FG}(\boldsymbol{\varphi})$ 中不成立。

若 $\varphi = 1_L$，取 $X_1 = \mathbf{Z}$，$\mathbf{Z}$ 为整数加法群，$X_2 = \mathbf{Q}$，$\mathbf{Q}$ 为有理数加法群，$A = X_1, B = X_2$，令

$$f: X_1 \to X_2$$
$$x \to x$$

则 f 是群同态，令 0 是 L 到 L 取常值 0 的映射，易见它保持任意并和任意交，且 $0^{-1} = \varphi_1$，则对 $\forall x \in X_1$，有

$$0^{-1}Bf(x) = 0^{-1}(B(f(x))) = 0^{-1}(B(x)) = 1 = A(x)$$

则有

$$A = 0^{-1}Bf$$

故 $(f,0) \in \hom(A,B)$ 在 $\mathbf{FG}(\mathbf{L})$ 中成立，但 $0 \neq 1_L$，所以 $\mathbf{FG}(\boldsymbol{\varphi})$ 不是 $\mathbf{FG}(\mathbf{L})$ 的完满子范畴。

上两个定理说明，普通群范畴 **Grp** 和 $\mathbf{FG}_0$ 的一个子范畴 $\mathbf{FG}_0(1_L)$ 同构，但不能与 $\mathbf{FG}(\mathbf{L})$ 的完满子范畴同构，从这里也看到，此处定义的 *CF* 群的同态映射与通常的定义不同。

定理 6.2.6 设 L_1 与 L_2 是两个同构的格，则 $FG(L_1)$ 与 $FG(L_2)$ 同构。

证 设 $\varepsilon: L_1 \to L_2$ 是格同构映射，在定理 6.2.2 的证明过程中已经指出，$\varepsilon^{-1}\varepsilon = 1_{L_1}$，从而也有 $\varepsilon\varepsilon^{-1} = 1_{L_2}$，做函子

$$\Phi: \mathbf{FG}(\mathbf{L}_1) \to \mathbf{FG}(\mathbf{L}_2)$$

使

$$\Phi: \mathrm{ob}\,\mathbf{FG}(\mathbf{L}_1) \to \mathrm{ob}\,\mathbf{FG}(\mathbf{L}_2)$$
$$A \to \varepsilon A$$
$$\hom(A,B) \to \hom(\Phi(A),\Phi(B))$$

$$(f,\varphi)\to(f,\varepsilon\varphi\varepsilon^{-1})$$

显然 $\Phi(A)\in$ ob $\mathbf{FG}(\mathbf{L}_2)$，又因为

$$\Phi(A)=\varepsilon A=\varepsilon\varphi^{-1}Bf=\varepsilon\varphi\varepsilon^{-1}\varepsilon Bf=(\varepsilon\varphi\varepsilon^{-1})\Phi(B)f$$

故 $\Phi(f,\varphi)\in\hom(\Phi(A),\Phi(B))$，而且

$$\Phi((g,\psi)(f,\varphi))=$$
$$\Phi(gf,\psi\varphi)=$$
$$(gf,\varepsilon\psi\varphi\varepsilon^{-1})=$$
$$(gf,\varepsilon\psi\varepsilon^{-1}\varepsilon\varphi\varepsilon^{-1})=$$
$$\Phi(g,\psi)\Phi(f,\varphi)$$

即

$$\Phi(1_X,1_{L_1})=(1_X,\varepsilon^{-1}\varepsilon_{L_1}\varphi)=(1_X,1_{L_2})$$

所以，Φ 确是 $\mathbf{FG}(\mathbf{L}_1)$ 到 $\mathbf{FG}(\mathbf{L}_2)$ 的函子。

做函子 $\Psi:\mathbf{FG}(\mathbf{L}_2)\to\mathbf{FG}(\mathbf{L}_1)$，使

$$\Psi:\text{ob }FG(L_2)\to\text{ob }FG(L_1)$$
$$B\to\varepsilon^{-1}B$$
$$\hom(A,B)\to\hom(\Psi(A),\Psi(B))$$
$$(f,\varphi)\to(f,\varepsilon^{-1}\varphi\varepsilon)$$

仿上易证，Ψ 确是函子。

又 $\quad\Phi\Psi(A)=\Phi(\varepsilon^{-1}A)=\varepsilon(\varepsilon^{-1}A)=A$

$$\Phi\Psi(f,\varphi)=\Phi(f,\varepsilon^{-1}\varphi\varepsilon)=(f,\varepsilon\varepsilon^{-1}\varphi\varepsilon\varepsilon^{-1})$$

故 $\Phi\Psi$ 是 $\mathbf{FG}(\mathbf{L}_2)$ 上的恒等函子，同理 $\Psi\Phi$ 是 $\mathbf{FG}(\mathbf{L}_1)$ 上的恒等函子，故 $\Phi^{-1}=\Psi$，Φ 是同构函子，$\mathbf{FG}(\mathbf{L}_1)$ 与 $\mathbf{FG}(\mathbf{L}_2)$ 同构。

定理 6.2.7 若 X_1 和 X_2 是两个同构的群，则 $\mathbf{FG}(\mathbf{X}_1)$ 与 $\mathbf{FG}(\mathbf{X}_2)$ 同构。

证 设 $h:X_1\to X_2$ 是群同构映射，做函子

$$G:\mathbf{FG}(\mathbf{X}_1)\to\mathbf{FG}(\mathbf{X}_2)$$

使得 $\quad G:\text{ob }\mathbf{FG}(\mathbf{X}_1)\to\text{ob }\mathbf{FG}(\mathbf{X}_2)$

$$A \to Ah^{-1}$$

$$\hom(A,B) \to \hom(G(A),G(B))$$

$$(f,\varphi) \to (hfh^{-1},\varphi)$$

易验证，G 是同构函子，故 $\mathbf{FG}(\mathbf{X}_1)$ 与 $\mathbf{FG}(\mathbf{X}_2)$ 同构。

设 X 是群，X 的所有子群加上空集组成的集合记为 $\mathscr{P}(X)$。

设 $A \in F_L(X)$，$\alpha \in L$，令

$$A\alpha = \{x \mid x \geqslant \alpha, x \in X\}$$

则 $A\alpha \in \mathscr{P}(X)$，且有如下性质

$$A_{\bigvee\limits_{i \in I} \alpha_i} = \bigcap_{i \in I} A_{\alpha_i}, A_0 = X$$

定理 6.2.8 （分解定理）

对任意 $A \in F_L(X)$，有 $A = \bigvee\limits_{\lambda \in L}(\lambda \wedge A_\lambda)$，此处 A_λ 理解为 A_λ 的特征函数，即

$$(\lambda \wedge A_\lambda)(x) = \begin{cases} \lambda, 若\ A(x) \geqslant \lambda \\ 0, 若\ A(x) < \lambda \end{cases}$$

定义 6.2.4 设 X 是群，X 的一个 L- 子群轮是一个映射 S: $L \to \mathscr{P}(X)$，满足下列条件：

(1) $S(\bigvee\limits_{i \in I}\alpha_i) = \bigcap\limits_{i \in I} S(\alpha_i)$，$\forall \{\alpha_i\}_{i \in I} \subset L$；

(2) $S(0) = X$。

X 的所有 L- 子群轮记做 $\mathscr{U}_L(X)$。

下面的定理给出了 CF 群的表现定理。

定理 6.2.9 映射 $\Phi: F_L(X) \to \mathscr{U}_L(X)$

$$A \to S: S(\alpha) = A_\alpha$$

是一一映射，且 $\Phi^{-1} = \Psi: \mathscr{U}_L(X) \to F_L(X)$

$$S \to A = \bigvee_{\lambda \in L}(\lambda \wedge S(\lambda))$$

其中 $S(\lambda)$ 理解为其特征函数，即

$$(\lambda \wedge S(\lambda))(x) = \begin{cases} \lambda, 若\ x \in S(\lambda) \\ 0, 若\ x \notin S(\lambda) \end{cases}$$

证 由模糊集的分解定理易得 $\Psi\Phi = 1_{F_L}(x)$，所以 Φ 是单射。再证 Φ 是满射，设 $S \in \mathscr{U}_L(X)$，令

$$I_x = \{\lambda \mid \lambda \in L, x \in S(\lambda)\}$$

$$A(x) = \bigvee_{\lambda \in I_x} \lambda = \bigvee_{\lambda \in L} (\lambda \wedge S(\lambda))(x) \quad (\forall x \in X)$$

下证 $I_x = [0, A(x)] = \{\lambda \mid \lambda \in L, \lambda \leqslant A(x)\}$。

由定义 6.2.4 的(1)，有

$$\lambda' \leqslant \lambda \Rightarrow S(\lambda) \subset S(\lambda')$$

故 $\lambda \in I_x$ 时，$x \in S(\lambda) \subset S(\lambda')$，从而 $\lambda' \in I_x$，即

$$\lambda \in I_x \Rightarrow [0, \lambda] \subset I_x$$

又因 $S(A(x)) = \bigcap_{\lambda \in I_x} S(\lambda)$，当 $\lambda \in I_x$ 时，$x \in S(\lambda)$，故

$$x \in S(A(x))$$

即 $A(x) \in I_x$，从而 $[0, A(x)] \subset I_x$。

反之，若 $\lambda \in I_x$，则 $\lambda \leqslant A(x)$，即 $\lambda \in [0, A(x)]$，所以

$$[0, A(x)] = I_x$$

若 $\lambda \in I_x \cap I_y$，则 $x \in S(\lambda)$，$y \in S(\lambda)$。因 $S(\lambda)$ 是子群，故 $xy \in S(\lambda)$，即 $\lambda \in I_{xy}$，故

$$I_x \cap I_y \subset I_{xy}$$

若 $\lambda \in I_x$，则 $x \in S(\lambda)$，由 $S(\lambda)$ 是子群，得 $x^{-1} \in S(\lambda)$，即 $\lambda \in I_{x^{-1}}$，故

$$I_x \subset I_{x^{-1}} \subset I_x = I_{(x^{-1})^{-1}}$$

但 $A(x) \wedge A(y) \in I_x \cap I_y \subset I_{xy} = [0, A(xy)]$，故

$$A(xy) \geqslant A(x) \wedge A(y)$$

$$A(x^{-1}) = A(x)$$

即 $A \in F_L(X)$，而且

$$A(x) \geqslant \lambda \Leftrightarrow \lambda \in I_x \Leftrightarrow x \in S(\lambda)$$

故 $A_\lambda = S(\lambda) \quad (\forall \lambda \in L)$，即 $S = \Phi(A)$。所以 Φ 是满射，且 Φ^{-1}

$= \Psi$。

定义 6.2.5 设 $S_1 \in \mathscr{U}_{L_1}(X_1)$，$S_2 \in \mathscr{U}_{L_2}(X_2)$，称 (f, φ) 是从 S_1 到 S_2 的同态映射，若 (f, φ) 满足定义 6.2.1 中的条件(1) 和(2)，且满足(3)，有

$$\bigvee_{\alpha \in L_1} (\alpha \wedge S_1(\alpha)) = \varphi^{-1} \bigvee_{\beta \in L_2} (\beta \wedge S_2(\beta)) f$$

从 S_1 到 S_2 的所有同态映射的集合记为 $\hom(S_1, S_2)$。

易得下面的定义。

定义 6.2.6 称 **FGU** 是一个 *CF* 群轮范畴，它的对象类为

$$\text{ob } \mathbf{FGU} = \{S \mid S \in \mathscr{U}_L(X)\}$$

对于 $S_1, S_2 \in \text{ob } \mathbf{FGU}$，$S_1, S_2$ 间的态射规定为定义 6.2.5 中的 $\hom(S_1, S_2)$，态射间的合成按定理 6.2.1 中的(a) 式规定。

定理 6.2.10 范畴 **FG** 与 **FGU** 同构，且有使态射不变的函子 E 存在。

证 如下定义的 E 就是使态射不变的同构函子

$$E: \text{ob } \mathbf{FG} \to \text{ob } \mathbf{FGU}$$

$$A \to S : S(\alpha) = A\alpha \quad (\forall \alpha \in L)$$

其中 $A \in F_L(X)$，$E(f, \varphi) = (f, \varphi)$。

其他可以直接验证，从略。

定义 6.2.7 **FGU(L)**，**FGU(X)**，**FGU(φ)** 和 $\mathbf{FGU}_0$ 都可以仿照定义 6.2.3 来定义。

定理 6.2.11 在定理 6.2.10 的同构函子 E 之下，**FG(L)**，**FG(X)**，**FG(φ)** 和 $\mathbf{FG}_0$ 分别同构于 **FGU** 的子范畴：**FGU(L)**，**FGU(X)**，**FGU(φ)** 和 $\mathbf{FGU}_0$

§6.3 *CLF* 群范畴

本节引入 *CLF* 群范畴的定义，指出上节的 *CF* 群范畴是本节

定义的子范畴，并证明 CLF 群范畴对乘积运算封闭，同时给出了 CLF 群范畴中的乘积的具体结构和一些性质。

首先引入几个概念。

定义 6.3.1 设 $X_1, X_2 \in \text{ob}\,\mathbf{Set}$，$\mathbf{CL}$ 表示以有最大元 1 和最小元 0 的完全分配格为对象，格同态为态射的范畴，$L_1, L_2 \in \text{ob}\,\mathbf{CL}$，$f \in \hom(X_1, X_2)$，$\varphi \in \hom(L_1, L_2)$，称映射

$$(f, \varphi): L_1^{X_1} \to L_2^{X_2}$$

为（f 和 φ 的）双诱导映射，如果 $\forall A \in L_1^{X_1}, B \in L_2^{X_2}$，有

$$(f,\varphi)(A)(x_2) = \bigvee_{f(x_1) = x_2} (\varphi(A(x_1))), x_1 \in X_1$$

称映射

$$(f, \varphi)^{-1}: L_2^{X_2} \to L_1^{X_1}$$

为 (f, φ) 的逆，如果 $\forall B \in L_2^{X_2}$，有

$$(f, \varphi)^{-1}(B) = \varphi^{-1} Bf$$

显然，若 $G_1, G_2 \in \text{ob}\,\mathbf{Grp}$，则有：

(1) 若 $A \in F_{L_1}(G_1) \Rightarrow (f, \varphi)(A) \in F_{L_2}(G_2)$；

(2) 若 $B \in F_{L_2}(G_2) \Rightarrow (f, \varphi)^{-1}(B) \in F_{L_1}(G_1)$。

命题 6.3.1 设 $X_1, X_2 \in \text{ob}\,\mathbf{Set}$，$L_1, L_2 \in \text{ob}\,\mathbf{CL}$，$\varphi \in \hom(L_1, L_2)$，$A \in L_1^{X_1}$，$B \in L_2^{X_2}$，则 $(f, \varphi)(A) \subseteq B$ 的充分必要条件是 $A \subseteq \varphi^{-1} Bf$。

证 必要性 若 $(f, \varphi)(A) \subseteq B$，则 $\forall x \in X_1$，有

$$\varphi(A(x)) \leqslant \bigvee_{f(x) = f(x_1)} (\varphi(A(x_1))), x_1 \in X_1$$

因而，$\varphi(A(x)) \leqslant (f, \varphi)(A)(f(x)) \leqslant B(f(x))$。

由定理 6.2.1 的证明中可得 $A(x) \leqslant \varphi^{-1}(B(f(x)))$，即 $A \subseteq \varphi^{-1} Bf$。

充分性 若 $A \subseteq \varphi^{-1} Bf$，则 $\forall x \in X_1, A(x) \leqslant \varphi^{-1}(B(f(x)))$，可以推出 $\varphi(A(x)) \leqslant B(f(x))$，故对 $\forall x_2 \in$

X_2，有

$$(f,\varphi)(A)(x_2)=\bigvee_{f(x)=x_2}(\varphi(A(x)))\leqslant \bigvee_{f(x)=x_2}(B(f(x)))= B(x_2)$$

故$(f,\varphi)(A)\subseteq B$。

定义 6.3.2 设$(L_1^{G_1},A)$，$(L_2^{G_2},B)$是 LF 群，$f\in \hom(G_1,G_2)$，$\varphi\in \hom(L_1,L_2)$，如果$(f,\varphi)(A)\subseteq B$(或$A\subseteq \varphi^{-1}Bf$)，则称$(f,\varphi)$是$(LG_1,A)$到$(L_2^{G_2},B)$的 CF 同态，并将$(L_1^{G_1},A)$到$(L_2^{G_2},B)$的所有 CF 同态的集合记做$\hom((L_1^{G_1},A),(L_2^{G_2},B))$。

显然，上节中的定义 6.2.1 是本定义的特例。

定义 6.3.3 设 **Grp** 表示群范畴，用 **CL** 表示以有最大元 1 和最小元 0 的完全分配格为对象，格同态为态射的范畴，CLF 群范畴 **FLG** 是指其对象类 ob **FLG** 为所有 LF 群构成的类，对于任意$(L_1^{G_1},A)$，$(L_2^{G_2},B)\in$ ob **FLG**，态射集

$$\hom((L_1^{G_1},A),(L_2^{G_2},B))\triangleq\{(f,\varphi)\mid (f,\varphi)\text{是}(L_1^{G_1},A)\text{到}(L_2^{G_2},B)\text{的 }CF\text{ 同态}\}$$

对于任意$(f,\varphi)\in \hom((L_1^{G_1},A),(L_2^{G_2},B))$，$(g,\psi)\in \hom((L_2^{G_2},B),(L_3^{G_3},C))$，态射的合成为$(g,\psi)(f,\varphi)=(gf,\psi\varphi)$。

可以验证上述定义是合理的。

需要指出的是，这里使用的范畴定义与上节的定义一致，即放弃了条件：

$$(A,B)\neq(C,D)\Rightarrow \hom(A,B)\cap \hom(B,C)\neq\varnothing$$

另外，上节的 CF 群范畴是本节中定义的 CLF 群范畴的子范畴，它们的对象类相同，态射集不同。

命题 6.3.2 若$\{(L^G,A),(f_i,\varphi_i)\mid i\in I\}$是 LF 群族

$\{(L_i^{G_i}, A_i)\}_{i\in I}$ 在范畴 **FLG** 中的乘积，则

(1) $\forall i \in I, (f_i, \varphi_i) \in \hom((L^G, A), (L_i^{G_i}, A_i))$ 是右可逆态射；

(2) $A = \bigcap_{i\in I} \varphi_i^{-1} A_i f_i$；

(3) $\{G, f_i \mid i \in I\}$ 是群族 $\{G_i\}_{i\in I}$ 在范畴 **Grp** 中的乘积；

(4) $\{L, \varphi_i \mid i \in I\}$ 是完全分配格族 $\{L_i\}_{i\in I}$ 在范畴 **CL** 中的乘积。

证 (1) 由于 $\{(L^G, A), (f_i, \varphi_i) \mid i \in I\}$ 是 LF 群族 $\{(L_i^{G_i}, A_i)\}_{i\in I}$ 在范畴 **FLG** 中的乘积，给定 $i \in I$，取 $(L^{*G^*}, B) = (L_i^{G_i}, A_i)$，$(g_i, \psi_i) = (1_{G_i}, 1_{L_i})$，并且当 $j \neq i$ 时，$(g_j, \psi_j) = (0_{G_j}, 0_{L_j})$，其中，$1_{G_i}, 1_{L_i}$ 分别是 G_i, L_i 上的恒等映射，$0_{G_j}(x) = e_j$，e_j 是 G_j 的单位元，$0_{L_j}(x) = 0$，0 是 L_j 的最小元。则 $\forall j \in I, (g_j, \psi_j) \in \hom((L^{*G^*}, B), (L_j^{G_j}, A_j))$，由经典范畴中积的定义（定义 5.5.2），存在同态映射 $(h, \pi) \in \hom((L^{*G^*}, B), (L^G, A))$，使得 $\forall j \in I, (f_j, \varphi_j)(h, \pi) = (g_j, \psi_j)$，特别地，$(f_i, \varphi_i)(h, \pi) = (1_{G_i}, 1_{L_i})$，所以 (f_i, φ_i) 是右可逆态射。

(2) 令 $A^* = \bigcap_{i\in I} \varphi_i^{-1} A_i f_i$，则 $A^* \in F_L(G)$，由 $\forall i \in I, (f_i, \varphi_i) \in \hom((L^G, A), (L_i^{G_i}, A_i))$，有 $\forall i \in I, A \subseteq \varphi_i^{-1} A_i f_i$，故 $A \subseteq \bigcap_{i\in I} \varphi_i^{-1} A_i f_i = A^*$。

次证 $A^* \subseteq A$。由于 $\{(L^G, A), (f_i, \varphi_i) \mid i \in I\}$ 是 LF 群族 $\{(L_i^{G_i}, A_i)\}_{i\in I}$ 的乘积，根据定义 5.5.2，对于 LF 群 (L^G, A^*) 和 $(f_i, \varphi_i) \in \hom((L^G, A^*), (L_i^{G_i}, A_i))$，存在惟一的同态 $(h, \pi) \in \hom((L^G, A^*), (L^G, A))$，使得 $\forall i \in I$，图 6-4 可交换，即 $\forall i \in I, (f_i, \varphi_i)(h, \pi) = (f_i, \varphi_i)$。由于 $A \subseteq A^*$，所以 $(1_G, 1_L) \in$

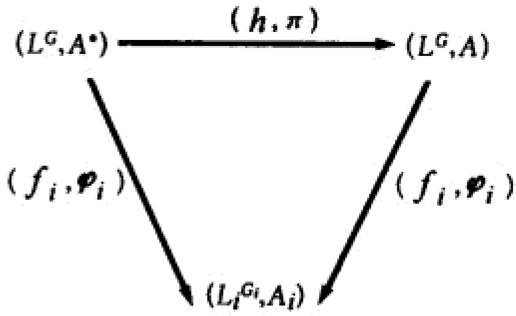


图 6-4

$\hom((L^G,A),(L^G,A^*))$，于是$(h,\pi)(1_G,1_L)\in\hom((L^G,A),(L^G,A))$，并且 $\forall i\in I$，有

$$(f_i,\varphi_i)[(h,\pi)(1_G,1_L)]=$$
$$[(f_i,\varphi_i)(h,\pi)](1_G,1_L)=$$
$$(f_i,\varphi_i)\circ(1_G,1_L)=(f_i,\varphi_i)$$

也就是对 $\forall i\in I$，图 6-5 可交换。根据定义 5.5.2 可知，仅有 $\hom((L^G,A),(L^G,A))$ 中的一个同态使图 6-5 可交换，并且 $(1_G,1_L)$ 也是这样的一个同态，所以$(h,\pi)(1_G,1_L)\in\hom((L^G,A^*),(L^G,A))$，于是 $A^*\subseteq A$。所以 $A=\bigcap_{i\in I}\varphi_i^{-1}A_if_i$。

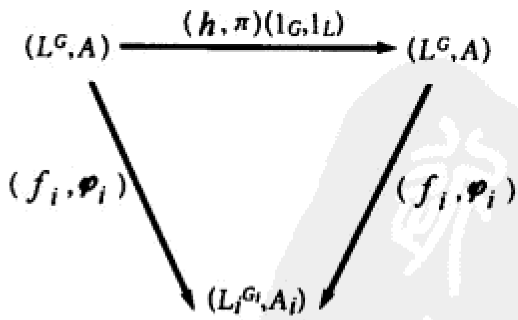


图 6-5

(3)，(4)　对于群 $G^*\in$ ob **Grp** 和群同态 $g_i\in\hom(G^*,G_i)$，以及完全分配格 $L^*\in$ ob **CL** 和格同态 $\psi_i\in\hom(L^*,L_i)$，

令 $B = \bigcap_{i \in I} \psi_i^{-1} A_i g_i$，则 $(L^{*G^*}, B) \in$ ob **FLG**，并且 $\forall i \in I$，$(g_i, \psi_i) \in \hom((L^{*G^*}, B), (L_i^{G_i}, A_i))$，由定义 5.5.2，存在惟一的 $(h, \pi) \in \hom((L^{*G^*}, B), (L^G, A))$，使得 $\forall i \in I$，图 6-6 可交换。也就

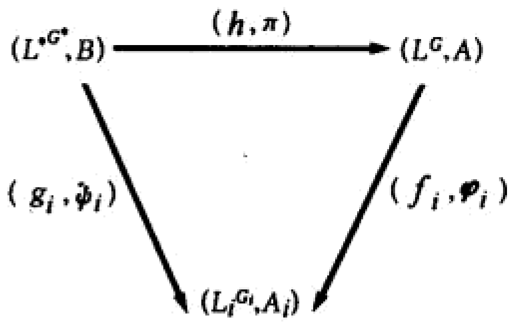


图 6-6

是 $\forall i \in I$，$(f_i, \varphi_i)(h, \pi) = (g_i, \psi_i)$，于是 $\forall i \in I$，$f_i h = g_i$，$\varphi_i \pi = \psi_i$，即 $\forall i \in I$，图 6-7 与图 6-8 可交换。若另有 $k \in \hom(G^*, G)$，$\theta \in \hom(L^*, L)$ 分别使图 6-7 和图 6-8 可交换，即 $\forall i \in I$，$f_i k = g_i$，$\varphi_i \theta = \psi_i$，则由

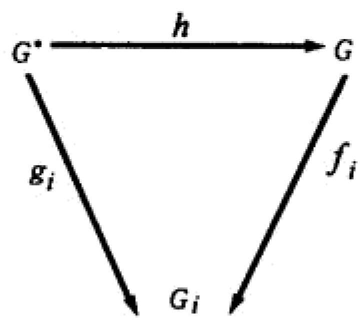


图 6-7

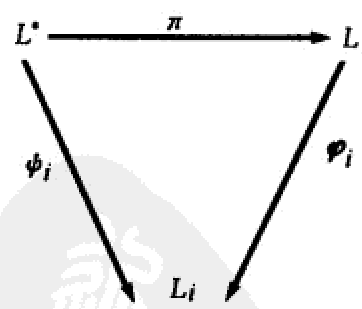


图 6-8

$$B = \bigcap_{i \in I} \psi_i^{-1} A_i g_i =$$

$$\bigcap_{i \in I} \theta^{-1} \varphi_i^{-1} A_i f_i k =$$

$$\theta^{-1} \left(\bigcap_{i \in I} \varphi_i^{-1} A_i f_i \right) k = \theta^{-1} A k$$

可知，$(k,\theta) \in \hom((L^{*G^*},B),(L^G,A))$，并且使得 $\forall i \in I$，$(f_i,\varphi_i)(k,\theta) = (g_i,\psi_i)$，即图 6-6 可交换。再由 (h,π) 的惟一性，$(h,\pi) = (k,\theta)$，所以 $h = k, \pi = \theta$，即分别使图 6-7 和图 6-8 可交换的 h 和 π 都是惟一的。所以 $\{G, f_i \mid i \in I\}$ 是群族 $\{G_i\}_{i\in I}$ 在范畴 **Grp** 中的乘积，$\{L, \varphi_i \mid i \in I\}$ 是完全分配格族 $\{L_i\}_{i\in I}$ 在范畴 **CL** 中的乘积。

命题 6.3.3 设 $\{(L_i^{G_i},A_i)\}_{i\in I}$ 是 LF 群族，如果 $\{G, f_i \mid i \in I\}$ 是群族 $\{G_i\}_{i\in I}$ 在范畴 **Grp** 中的乘积，$\{L, \varphi_i \mid i \in I\}$ 是完全分配格族 $\{L_i\}_{i\in I}$ 在范畴 **CL** 中的乘积，令 $A = \bigcap_{i\in I}\varphi_i^{-1}A_if_i$，则 $\{(L^G, A),(f_i,\varphi_i) \mid i \in I\}$ 是 LF 群族 $\{(L_i^{G_i},A_i)\}_{i\in I}$ 在范畴 **FLG** 中的乘积。

证 设 $(L^{*G^*},B) \in$ ob **FLG**，$(g_i,\psi_i) \in \hom((L^{*G^*},B),(L_i^{G_i},A_i))$，$i \in I$，则 $G^* \in$ ob **Grp**，$g_i \in \hom(G^*,G_i)$，$L^* \in$ ob **CL**，$\psi_i \in \hom(L^*,L_i)$。因为 $\{G, f_i \mid i \in I\}$ 是群族 $\{G_i\}_{i\in I}$ 在范畴 **Grp** 中的乘积，$\{L, \varphi_i \mid i \in I\}$ 是完全分配格族 $\{L_i\}_{i\in I}$ 在范畴 **CL** 中的乘积，由定义 5.5.2，存在惟一的群同态 $h \in \hom(G^*, G)$ 与惟一的格同态 $\pi \in \hom(L^*,L)$，使得 $\forall i \in I$，图 6-9 与图 6-10 可交换，也就是 $f_ih = g_i$，$\varphi_i\pi = \psi_i$。由于 $(g_i,\psi_i) \in$

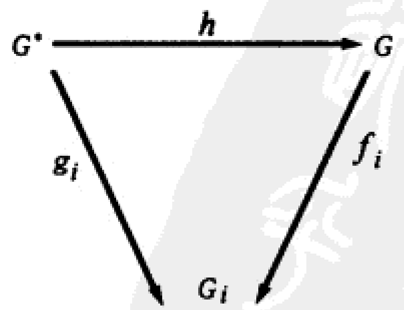


图 6-9

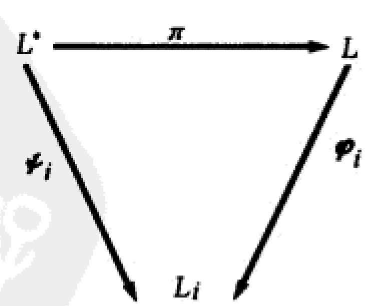


图 6-10

$\hom((L^{*G^*},B),(L_i^{G_i},A_i))$，所以 $B\subseteq \psi_i^{-1}A_ig_i$，于是

$$\begin{aligned}B\subseteq\bigcap_{i\in I}\psi_i^{-1}A_ig_i &= \\ \bigcap_{i\in I}(\varphi_i\pi)^{-1}A_i(f_ih) &= \\ \bigcap_{i\in I}\pi^{-1}\varphi_i^{-1}A_if_ih &= \\ \pi^{-1}(\bigcap_{i\in I}\varphi_i^{-1}A_if_i)h &= \\ \pi^{-1}Ah\end{aligned}$$

因此 $(h,\pi)\in\hom((L^{*G^*},B),(L^G,A))$，并且使得 $(f_i,\varphi_i)(h,\pi)=(g_i,\psi_i)$，即图 6-11 可交换。

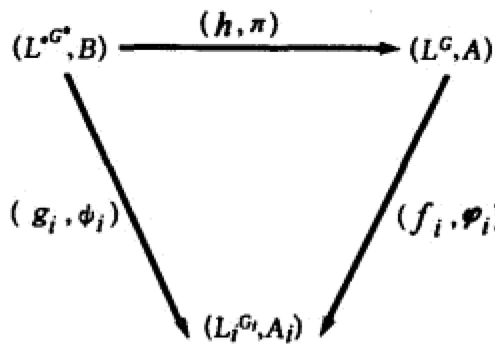


图 6-11

如果另有同态 $(k,\theta)\in\hom((L^{*G^*},B),(L^G,A))$，使得 $(f_i,\varphi_i)(k,\theta)=(g_i,\psi_i)$，$i\in I$，即图 6-11 可交换，则 $f_ik=g_i$，$\varphi_i\theta=\psi_i$，即群同态 $k\in\hom(G^*,G)$，格同态 $\theta\in\hom(L^*,L)$ 分别使上述图 6-9 和图 6-10 可交换。再由 h 与 π 的惟一性可知，$h=k$，$\pi=\theta$，所以 $(h,\pi)=(k,\theta)$。由定义 5.5.2，$\{(L^G,A),(f_i,\varphi_i)\mid i\in I\}$ 是 LF 群族 $\{(L_i^{G_i},A_i)\}_{i\in I}$ 在范畴 **FLG** 中的乘积。

由上述结果可以直接推出以下命题。

命题 6.3.4 $\{(L^G,A),(f_i,\varphi_i)\mid i\in I\}$ 是 LF 群族 $\{(L_i^{G_i},A_i)\}_{i\in I}$ 在范畴 **FLG** 中的乘积当且仅当 $\{G,f_i\mid i\in I\}$ 是群族

$\{G_i\}_{i\in I}$ 在范畴 Grp 中的乘积，$\{(L,\varphi_i)\mid i\in I\}$ 是完全分配格族 $\{L_i\}_{i\in I}$ 在范畴 CL 中的乘积，并且 $A=\bigcap_{i\in I}\varphi_i^{-1}A_if_i$。

以下我们讨论，任意一族 LF 群在范畴 FLG 中的乘积存在。

设 $\{(L_i^{G_i},A_i)\}_{i\in I}$ 是一族 LF 群，$\{P_i\}_{i\in I}$ 是自然投射族，即 $\forall i\in I$

$$P_i:\prod_{i\in I}G_i\to G_i$$

$$P_i(\{x_i\}_{i\in I})=x_i$$

$$P_i:\prod_{i\in I}L_i\to L_i$$

$$P_i(\{a_i\}_{i\in I})=a_i$$

则 $\{\prod_{i\in I}G_i,P_i\mid i\in I\}$ 是群族 $\{G_i\}_{i\in I}$ 在范畴中 Grp 的一个乘积，$\{\prod_{i\in I}L_i,P_i\mid i\in I\}$ 是完全分配格族 $\{L_i\}_{i\in I}$ 在范畴 CL 中的一个乘积。

对于任意 $\{x_i\}_{i\in I}\in\prod_{i\in I}G_i$，令

$$A(\{x_i\}_{i\in I})=\{A_i(x_i)\}_{i\in I}\in\prod_{i\in I}L_i$$

则
$$A=\bigcap_{i\in I}P_i^{-1}A_iP_i$$

由命题 6.3.4，$\left\{(\prod_{i\in I}L^{\prod_{i\in I}G_i},A),(P_i,P_i)\mid i\in I\right\}$ 是 LF 群族 $\{(L_i^{G_i},A_i)\}_{i\in I}$ 在范畴 FLG 中的一个乘积，我们将 $(\prod_{i\in I}L^{\prod_{i\in I}G_i},A)$ 记做 $\prod_{i\in I}(L_i^{G_i},A_i)$，于是得到以下结论。

命题 6.3.5 对于任意一族 LF 群 $\{(L_i^{G_i},A_i)\}_{i\in I}$，$\{\prod_{i\in I}(L_i^{G_i},A_i),(P_i,P_i)\mid i\in I\}$ 是该族在范畴 FLG 中的一个乘积。

下面讨论这个乘积的性质。

命题 6.3.6 设 $\sigma:I\to I$ 是双射，则存在同构

$$\prod_{i\in I}(L_i^{G_i},A_i)\cong\prod_{i\in I}(L_{\sigma(i)}^{G_{\sigma(i)}},A_{\sigma(i)})$$

其中 $\cong$ 表示范畴中对象之间的同构关系。

证 只需注意到 $\{\prod_{i\in I}(L_{\sigma(i)}^{G_{\sigma(i)}},A_{\sigma(i)}),(P_{\sigma(i)},P_{\sigma(i)})\,\big|\,i\in I\}$ 是 LF 群族 $\{(L_i^{G_i},A_i)\}_{i\in I}$ 在范畴 **FLG** 中的一个乘积,即得结论。

命题 6.3.7 对于 I 的一个任意划分 $\{I_j\mid_{j\in J}\}$,存在同构

$$\prod_{i\in J}(L_i^{G_i},A_i)\cong\prod_{j\in J}(\prod_{i\in I_j}(L_i^{G_i},A_i))$$

证 只需证明 $\{\prod_{j\in J}(\prod_{i\in I_j}(L_i^{G_i},A_i)),(P_i,P_i)(P_j,P_j)\mid i\in I_j,j\in J\}$ 是 LF 群族 $\{(L_i^{G_i},A_i)\}_{i\in I}$ 在范畴 **FLG** 中的一个乘积。设 $(L^{*G^*},B)\in \mathrm{ob}\,\mathbf{FLG}$,$(g_i,\psi_i)\in\hom((L^{*G^*},B),(L_i^{G_i},A_i))$,$\forall i\in I$,令 $j\in J$,使得 $i\in I_j$,于是,在图 6-12 中,存在惟一的

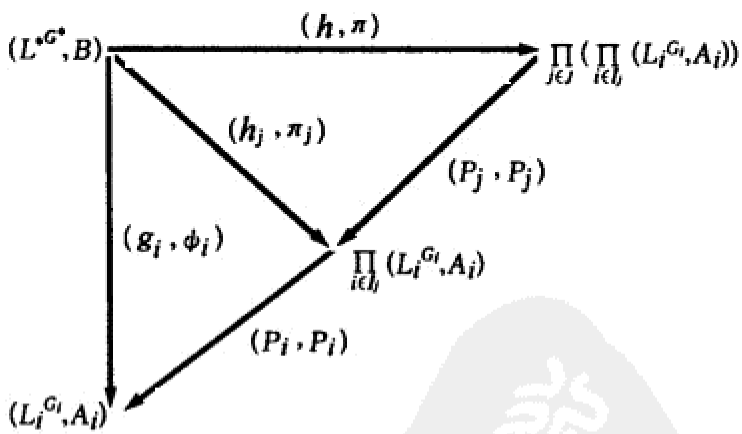


图 6-12

$(h_j,\pi_j)\in\hom((L^{*G^*},B),(L_i^{G_i},A_i))$,使得 $(P_i,P_i)(h_j,\pi_j)=(g_i,\psi_i)$,$i\in I_j$,以及惟一的同态 $(h,\pi)\in\hom((L^{*G^*},B),\prod_{j\in J}(\prod_{i\in I_j}(L_i^{G_i},A_i)))$,使得 $(P_j,P_j)(h,\pi)=(h_j,\pi_j)$,$j\in J$,由此可得 $(P_i,P_i)(P_j,P_j)(h,\pi)=(g_i,\psi_i)$,$i\in I_j$,$j\in J$。

若另有同态$(k,\theta)\in \hom((L^{\bullet G^{\bullet}},B),\prod_{j\in J}(\prod_{i\in I_j}(L_i^{G_i},A_i)))$，使得图 6-12 中最大的三角形可交换，则

$$(P_i,P_i)(P_j,P_j)(k,\theta)=(g_i,\psi_i),i\in I_j,j\in J$$

于是

$$(P_i,P_i)(P_j,P_j)(h,\pi)=(P_i,P_i)(P_j,P_j)(k,\theta)$$

可知$(h,\pi)=(k,\theta)$，故

$$\{\prod_{j\in J}(\prod_{i\in I_j}(L_i^{G_i},A_i)),(P_i,P_i)(P_j,P_j)\mid i\in I_j,j\in J\}$$

是 *LF* 群族$\{(L_i^{G_i},A_i)\}_{i\in I}$在范畴 **FLG** 中的一个乘积。

§6.4 *CLF* 模范畴

本节用 R 表示一个单位元 1_R 的环，**Mod-R** 表示右 R- 模范畴。**R-Mod** 表示左 R- 模范畴，**Ab** 表示 Abel 群范畴，显然，**Ab** = **Z-Mod** = **Mod-Z**，其中 **Z** 是整数环。

定义 6.4.1 设 L 是有最大元 1 和最小元 0 的完全分配格，$M\in$ ob **Mod-R**，A 是 M 的 L 模糊子集，如果：

(1)$A(0_M)=1$；

(2)$A(x)\wedge A(y)\leqslant A(x+y)$；

(3)$A(x)\leqslant A(-x)$；

(4)$A(x)\leqslant A(xr)$。

其中 $x,y\in M,r\in R,0_M$ 是 M 中的零元素，则称 A 是 M 的 *LF* 右 R- 子模。类似地，可以定义 *LF* 左 R- 模和 *LF* Abel 群。

右 R- 子模 M 的所有 *LF* 右 R- 子模构成的类记做 $F(M)$。

定理 6.4.1 设 $A_i\in F(M),i\in I$，则：

(1) $\bigcap_{i\in I}A_i\in F(M)$；

(2) $\bigoplus_{i\in I}A_i\in F(M)$。

其中

$$(\bigoplus_{i\in I}A_i)(x)=\bigvee\{\bigwedge_{1\leqslant k\leqslant p}A_{i_k}(x_k)\mid\sum_{k=1}^{p}x_k=x,$$
$$x_k\in M,p\in\mathbf{Z}^+,i_k\in I\}$$

证明属验证性的,略。

定义 6.4.2 设 $M\in$ ob **Mod-R**, $A\in L^M$,令

$$\langle A\rangle=\bigcap\{B\mid A\subseteq B,B\in F(M)\}$$

由定理6.4.1, $\langle A\rangle\in F(M)$,称 $\langle A\rangle$ 为由 A 生成的 M 的 LF 右 R-子模。

定理 6.4.2 设 $M\in$ ob **Mod-R**, $A\in L^M$, $x\in M$,则

$$\langle A\rangle(x)=\bigvee(\bigwedge_{1\leqslant k\leqslant p}A(x_k)\mid\sum_{k=1}^{p}x_k=x,$$
$$p\in\mathbf{Z}^+,x_k\in M)$$

证 设 $C\in L^M$,并且

$$C(x)=\bigvee(\bigwedge_{1\leqslant k\leqslant p}A(x_k)\mid\sum_{k=1}^{p}x_k=x,$$
$$p\in\mathbf{Z}^+,x_k\in M)$$

易证 $C\in F(M)$,由于

$$A(x)\leqslant\bigvee(\bigwedge_{1\leqslant k\leqslant p}A(x_k)\mid\sum_{k=1}^{p}x_k=x,$$
$$p\in\mathbf{Z}^+,x_k\in M)=C(x)$$

故 $A\subseteq C$,所以 $\langle A\rangle\subseteq C$。其次,设 $A\subseteq B\in F(M)$,则

$$C(x)=\bigvee(\bigwedge_{1\leqslant k\leqslant p}A(x_k)\mid\sum_{k=1}^{p}x_k=x,$$
$$p\in\mathbf{Z}^+,x_k\in M)\leqslant$$
$$\bigvee(\bigwedge_{1\leqslant k\leqslant p}B(x_k)\mid\sum_{k=1}^{p}x_k=x,$$

$$p \in \mathbf{Z}^+, x_k \in M) \leqslant$$

$$\vee (B(\sum_{k=1}^{p} x_k) \Big| \sum_{k=1}^{p} x_k = x,$$

$$p \in \mathbf{Z}^+, x_k \in M) = B(x)$$

即 $C \subseteq B$，所以

$$C \subseteq \cap \{B \mid A \subseteq B \in F(M)\} = \langle A \rangle$$

因此 $\langle A \rangle = C$。

给定通常映射 $f: X \to Y$，并记 $f: L^X \to L^Y$ 为由 Zadeh 的扩展原理得到的模糊型映射，即 $\forall A \in L^X, y \in Y, f(A)(y) = \vee \{A(x) \mid x \in X, f(x) = y\}$，又记 $f^{-1}: L^Y \to L^X$，其中 $\forall B \in L^Y, f^{-1}(B) = Bf$，这里约定空集 $\varnothing$ 的上确界等于零。

定理 6.4.3 设 $f: X \to Y$ 是通常映射，并且 $A \in L^X, B \in L^Y$，则 $f(A) \subseteq B$，当且仅当 $A \subseteq Bf$。

定义 6.4.3 设 $(X, A), (Y, B)$ 是 LF 集，$f: X \to Y$ 是通常映射，如果 $f(A) \subseteq B$（或 $A \subseteq Bf$），则称 f 是 (X, A) 到 (Y, B) 的 LF 集映射，记做 $f: (X, A) \to (Y, B)$。

定理 6.4.4 设 $f: M \to N$ 是右 R- 模同态，则：

(1) 若 $A \in F(M)$，则 $f(A) \in F(N)$；

(2) 若 $B \in F(N)$，则 $f^{-1}(B) \in F(M)$。

定理 6.4.5 设 $f: M \to N$ 是右 R- 模同态，$A \in L^M$，则 $f(\langle A \rangle) = \langle f(A) \rangle$。

证 由 $A \subseteq \langle A \rangle$ 可知 $f(A) \subseteq f(\langle A \rangle)$，由定理 6.4.4，$f(\langle A \rangle) \in F(N)$，所以 $\langle f(A) \rangle \subseteq f(\langle A \rangle)$。其次，由

$$\langle f(A) \rangle = \cap \{C \mid f(A) \subseteq C, C \in F(N)\}$$

$$f(\langle A \rangle) = f(\cap \{B \mid A \subseteq B, B \in F(M)\}) \subseteq$$

$$\cap \{f(B) \mid A \subseteq B, B \in F(M)\}$$

任取 $C_0 \in \{C \mid f(A) \subseteq C, C \in F(N)\}$，令 $B_0 = C_0 f$，则由定理

6.4.4, $B_0 \in F(M)$。由 $f(A) \subseteq C_0$ 可知 $A \subseteq C_0 f = B_0$，于是 $f(B_0) \in \{f(B) \mid A \subseteq B, B \in F(M)\}$，再由 $B_0 = C_0 f$ 可知 $f(B_0) \subseteq C_0$，所以 $\bigcap \{f(B) \mid A \subseteq B, B \in F(M)\} \subseteq \{C \mid f(A) \subseteq C, C \in F(N)\}$，可知 $f(\langle A \rangle) \subseteq \langle f(A) \rangle$。因此 $f(\langle A \rangle) = \langle f(A) \rangle$。

定义6.4.4 设 A, B 分别是 M 和 N 的 LF 右 R- 子模，$f: M \to N$ 是右 R- 模同态，如果 $f(A) \subseteq B$（或 $A \subseteq Bf$），则称 f 是 (M, A) 到 (N, B) 的 LF 右 R- 模同态，记做 $f: (M, A) \to (N, B)$。

定义6.4.5 CLF 右 R- 模范畴[①]**FMod-R** 是指：对象类为所有 LF 右 R- 子模构成的类，对于 $(M, A), (N, B) \in$ ob **FMod-R**，态射集

$$\hom_{\mathbf{FMod\text{-}R}}((M, A), (N, B)) = \{f \mid f: (M, A) \to (N, B) \text{ 是 } LF \text{ 右 } R\text{- 模同态}\}$$

态射的合成由右 R- 模同态的合成所决定。

同样，可以定义 CLF 左 R- 模范畴 **R-FMod**，并且，定义 CLF Abel 群范畴 **FAb** $\triangleq$ **FMod-Z** $\triangleq$ **Z-FMod**。

设 $(M, A) \in$ ob **FMod-R**，$(N, B) \in$ ob **R-FMod**，(M, A) 与 (N, B) 的乘积是指 LF 集合 $(M \times N, A \times B)$，其中，$M \times N$ 是 M 与 N 的笛卡儿乘积，对于 $(x, y) \in M \times N$，$(A \times B)((x, y)) = A(x) \wedge B(y)$，该乘积记做 $(M, A) \times (N, B)$。

设 $(M, A) \in$ ob **FMod-R**，$(N, B) \in$ ob **R-FMod**，(M, A) 与 (N, B) 的平衡乘积是指偶序 $((P, C), f)$，其中 $(P, C) \in$ ob **FAb**，$f: M \times N \to P$ 是通常映射，并且满足以下条件：

(1) (P, f) 是经典代数中 M 与 N 的平衡乘积；

(2) f 是 $(M, A) \times (N, B)$ 到 (P, C) 的 LF 集映射。

---

① 汤建钢. L-Fuzzy 模范畴的张量积与张量函子. 模糊系统与数学, 1995(3): 65 ~ 73

根据 Zadeh 扩展原理，由映射 $f:M\times N\to P$ 可以诱导出映射 $f:L^M\times L^N\to L^P$，其中 $f(A,B)(z)=\vee\{A(x)\wedge B(y)\mid x\in M,y\in N,f(x,y)=z\}$，这样，$f$ 是 $(M,A)\times(N,B)$ 到 (P,C) 的 LF 集映射当且仅当 $f(A,B)\subseteq C$。

定义 6.4.6 设

$$(M,A)\in \text{ob}\ \mathbf{FMod\text{-}R},(N,B)\in \text{ob}\ \mathbf{R\text{-}FMod}$$

(M,A) 与 (N,B) 的张量积指平衡乘积 $((T,C),f)$，使得对于 (M,A) 与 (N,B) 的任意平衡乘积 $((P,D),g)$，存在惟一的 $h\in \hom_{\mathbf{FAb}}((T,C),(P,D))$，使得图 6-13 可交换。

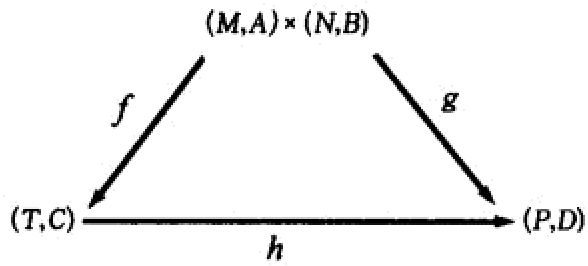


图 6-13

下面给出 CLF 模的张量积的结构定理。

定理 6.4.6 设

$$(M,A)\in \text{ob}\ \mathbf{FMod\text{-}R}(N,B)\in \text{ob},\mathbf{R\text{-}FMod}$$

则有 $((T,C),f)$ 是 (M,A) 与 (N,B) 的张量积，当且仅当：

(1) (T,f) 是 M 与 N 的张量积；

(2) $C=\langle f(A,B)\rangle$。

证 必要性 (1) 由于 $((T,C),f)$ 是 (M,A) 与 (N,B) 的张量积，所以 (T,f) 是 M 与 N 的平衡乘积。设 (P,g) 是 M 与 N 的一个平衡乘积，令 $D=\langle g(A,B)\rangle$，则 $((P,D),g)$ 是 (M,A) 与 (N,B) 的平衡乘积。因 $((T,C),f)$ 是 (M,A) 与 (N,B) 的张量积，由定义 6.4.6，存在惟一的 $h\in \hom_{\mathbf{FAb}}((T,C),(P,D))$，使得

$hf = g$，于是 $h \in \hom_{Ab}(T,P)$，使得 $hf = g$。

下面证明满足 $hf = g$ 的 $h \in \hom_{Ab}(T,P)$ 是惟一的。为此，设 $j \in \hom_{Ab}(T,P)$，使得

$$jf = g$$

则

$$\begin{aligned} j(C) = & j(\langle f(A,B)\rangle) = \\ & \langle j(f(A,B))\rangle = \\ & \langle g(A,B)\rangle = D \end{aligned}$$

可知

$$j \in \hom_{FAb}((T,C),(P,D))$$

并且满足 $jf = g$，由于在定义 6.4.6 中满足条件的 $h \in \hom_{FAb}((T,C),(P,D))$ 是惟一的，故 $h = j$，所以 (T,f) 是 M 与 N 的张量积。

(2) 令 $C^* = \langle f(A,B)\rangle$，因 $f(A,B) \subseteq C$，并且 $C \in F(T)$，由定义 6.4.2，$C^* = \langle f(A,B)\rangle \subseteq C$。

在定义 6.4.6 中，取 $((P,D),g) = ((T,C^*),f)$，则 $((T,C^*),f)$ 是 (M,A) 与 (N,B) 的平衡乘积，于是存在惟一的 $h \in \hom_{FAb}((T,C),(T,C^*))$，使得 $hf = f$，由于 $C^* \subseteq C$，故 $1_T(C^*) \subseteq C$，其中 1_T 是 T 上的恒同映射，所以 $1_T \in \hom_{FAb}((T,C^*),(T,C))$，于是 $1_T h \in \hom_{FAb}((T,C),(T,C))$，并且 $(1_T h)f = 1_T(hf) = 1_F f = f$。

另外，$1_T \in \hom((T,C),(T,C))$，同样使 $1_T f = f$，在定义 6.4.6 中，取 (M,A) 与 (N,B) 的平衡乘积 $((P,D),g) = ((T,C),f)$，由惟一性，$1_T h = 1_T$，所以 $h = 1_T$，再由 $h \in \hom_{FAb}((T,C),(T,C^*))$，可知 $C = 1_T(C) \subseteq C^*$，所以 $C = C^*$，即 $C = \langle f(A,B)\rangle$。

充分性　设 $((P,D),g)$ 是 (M,A) 与 (N,B) 的平衡乘积，

则(P,g)是M与N的平衡乘积，因为(T,f)是M与N的张量积，由经典代数中张量积的定义，存在惟一的$h \in \hom_{Ab}(T,P)$，使得$hf = g$，由于$g(A,B) \subseteq D$，故$\langle g(A,B)\rangle \subseteq D$，于是$h(C) = h(\langle f(A,B)\rangle) = \langle h(f(A,B))\rangle = \langle g(A,B)\rangle = D$，所以$h \in \hom_{FAb}((T,C),(P,D))$，并且使$hf = g$，而$h$的惟一性是显然的，所以$((T,C),f)$是$(M,A)$与$(N,B)$的张量积。

我们进一步指出，在同构的意义下，这样的张量积是惟一的。

定理 6.4.7 设$((T,C),f)$是(M,A)与(N,B)的张量积，则$((T',C'),f')$也是(M,A)与(N,B)的张量积当且仅当存在同构态射$h \in \hom_{FAb}((T,C),(T',C'))$，使得$hf = f'$。

证 在定义 6.4.6 中，取

$$((P,D),g) = ((T',C'),f')$$

则存在

$$h \in \hom_{FAb}((T,C),(T',C'))$$

使得$hf = f'$，类似地，存在

$$j \in \hom_{FAb}((T',C'),(T,C))$$

使得$jf' = f$，考虑到

$$jh \in \hom_{FAb}((T,C),(T,C))$$
$$1_T \in \hom_{FAb}((T,C),(T,C))$$

并且

$$(jh)f = j(hf) = jf' = f$$
$$1_T f = f$$

在定义 6.4.6 中，取平衡乘积$((P,D),g) = ((T,C),f)$，则由惟一性

$$jh = 1_T$$

同理可证$hj = 1_{T'}$，因此$h \in \hom_{FAb}((T,C),(T',C'))$是同构态射，且使$hf = f'$。

另一方面，若存在同构态射

$$h \in \hom_{FAb}((T,C),(T',C'))$$

使 $hf = f'$，则存在

$$k \in \hom_{FAb}((T',C'),(T,C))$$

使得 $kh = 1_T, hk = 1_{T'}$，于是

$$kf' = f$$

对于(M,A)与(N,B)的平衡乘积$((P,D),g)$，由定义6.4.6，存在惟一的 $l \in \hom_{FAb}((T,C),(P,D))$，使得

$$lf = g$$

于是

$$lk \in \hom_{FAb}((T',C'),(P,D))$$

使得

$$(lk)f' = l(kf') = lf = g$$

以下证明满足该条件的 lk 惟一。若另有

$$t \in \hom_{FAb}((T',C'),(T,C))$$

使得 $tf' = g$，则

$$th \in \hom_{FAb}((T,C),(P,D))$$

并且使得

$$(th)f = t(hf) = tf' = g$$

再由 l 的惟一性可知，$l = th$。于是

$$t = lk$$

惟一性得证。

§6.5 *CLF* 拓扑群范畴

设 G 是一个群，L 是一个格，(G,δ) 为格上的 Fuzzy 拓扑空间，简记为 LF 拓扑空间，LF 映射同上节一样是由扩展原理得到

的模糊型映射。

令 $A,B\in L^G$,定义

$$AB(x)=\bigvee_{x=x_1x_2}(A(x_1)\wedge B(x_2)),A^{-1}(x)=A(x^{-1})$$

定义 6.5.1 设 G 是群,(G,δ) 为 LF 拓扑空间,若下述条件被满足:

(1) 映射 $f:(G,\delta)\times(G,\delta)\to(G,\delta)$

$$(x,y)\to xy$$

是 LF 连续的;

(2) 映射 $g:(G,\delta)\to(G,\delta)$

$$x\to x^{-1}$$

是 LF 连续的。

则称 G 是 LF 拓扑群①。

定义 6.5.2 若 f 是 LF 连续映射,且诱导 f 的分明映射 f_c:$G_1\to G_2$ 是群同态,则称 f 是 LF 连续同态。

定义 6.5.3 LF 拓扑群(G,δ)称为诱导 LF 拓扑群,若 LF 拓扑 δ 是由某个分明拓扑诱导出来的。

由范畴的定义,直接推出下面的命题。

命题 6.5.1 (1) 以 LF 拓扑群为对象,以 LF 连续同态为态射形成一个范畴,记为 **FTG**,称为 CLF 拓扑群范畴②。

(2) 以诱导 LF 拓扑群为对象,以 LF 连续同态为态射形成一个范畴,记为 **FITG**,称为诱导 CLF 拓扑群范畴。

显然,**FITG** 是 **FTG** 的满子范畴。

用 **TG** 表示分明拓扑群范畴,则有以下定义。

定义 6.5.4 令 $\omega_L:\mathbf{TG}\to\mathbf{FTG}$

$$\forall(G,\tau)\in \mathrm{ob}\,\mathbf{TG},\omega_L(G,\tau)=(G,\omega_L(\tau))$$

---

① 郭开其. Fuzzy 拓扑群的一些性质. 模糊数学,1982(3):1～6

② 周相泉. L-Fuzzy 拓扑范畴. 烟台大学学报,1998(2):85～90

$$\forall f_c \in \hom_{TG}((G_1,\tau_1),(G_2,\tau_2)), \omega_L(f_c) = f$$

这里 $f:(G_1,\omega_L(\tau_1)),(G_2,\omega_L(\tau_2))$ 是由分明映射 f_c 诱导的 LF 映射，则称 ω_L 是一函子，它把 TG 嵌入成 FTG 的满子范畴 FITG。

再来构造 ω_L 的右伴随。

定理 6.5.1 若$(G,\delta) \in$ ob **FTG**，则$(G,l_L(\delta)) \in$ ob **TG**。

证 $\forall x,y \in G, \forall V \in N(xy^{-1})$，$N(xy^{-1})$ 表示 xy^{-1} 的开邻域系，$\exists r_i \in P(L)$，$P(L)$ 表示 L 的全体非1素元，$A_i \in \delta, i = 1,2,\cdots,n$，使 $xy^{-1} \in \bigcap_{i=1}^{n} l_{r_i}(A_i) \subset V$，从而，$\forall i, A_i(xy^{-1}) \nleq r_i$，于是 $A_i' \in \eta((xy^{-1})_{r_i'})$，此处 $\eta((xy^{-1})_{r_i'})$ 表示模糊点$(xy^{-1})_{r_i'}$ 的模糊开邻域系。由$(G,\delta) \in$ ob **FTG**，$\exists Q_i \in \eta(x_{r_i'})$ 及 $R_i \in \eta(y_{r_i'})$，使 $A_i' \subseteq (Q_i'(R_i^{-1})')'$，$i = 1,2,\cdots,n$，因而 $x \in l_{r_i}(Q_i') \in N(x), y \in l_{r_i}(R_i') \in N(y), i = 1,2,\cdots,n$。设 $V_1 = \bigcap_{i=1}^{n} l_{r_i}(Q_i'), V_2 = \bigcap_{i=1}^{n} l_{r_i}(R_i')$，则 $V_1 \in N(x), V_2 \in N(y)$。另外，由 $A_i \supseteq Q_i'(R_i^{-1})'$ 得 $l_{r_i}(A_i) \supset l_{r_i}(Q_i'(R_i^{-1})'), i = 1,2,\cdots,n$，于是

$$\begin{aligned} V_1 V_2^{-1} = {} & (\bigcap_{i=1}^{n} l_{r_i}(Q_i'))(\bigcap_{i=1}^{n} l_{r_i}(R_L'))^{-1} = \\ & (\bigcap_{i=1}^{n} l_{r_i}(Q_i'))(\bigcap_{i=1}^{n} l_{r_i}(R_i^{-1})') \subset \\ & \bigcap_{i=1}^{n} l_{r_i}(Q_i') l_{r_i}((R_i^{-1})') \subset \\ & \bigcap_{i=1}^{n} l_{r_i}(Q_i'(R_i^{-1})') \subset \\ & \bigcap_{i=1}^{n} l_{r_i}(A_i) \subset V \end{aligned}$$

所以$(G,l_L(\delta)) \in$ ob **TG**。

命题 6.5.2 设(G_i,δ_i)，$i=1,2$，是 LF 拓扑群，且 $f:(G_1,\delta_1)\rightarrow(G_2,\delta_2)$ 是 LF 连续映射，则诱导 f 的分明映射 f_c 是从$(G_1,l_L(\delta_1))$到$(G_2,l_L(\delta_2))$的连续映射。

证 设 $\varphi(\delta_2)=\{l_r(B):B\in\delta_2,r\in P(L)\}$ 是$(G_2,l_L(\delta_2))$ 的子基，$\forall\, l_r(B)\in\varphi(\delta_2)$。容易验证，$f_c^{-1}(l_r(B))=l_r(f^{-1}(B))$。由 $f^{-1}(B)\in\delta_1$ 得 $f_c^{-1}(l_r(B))\in l_L(\delta_1)$，所以 f_c 是分明连续映射。

定理 6.5.2 令 $l_L:\mathbf{FTG}\rightarrow\mathbf{TG}$

$$\forall(G,\delta)\in \mathrm{ob}\,\mathbf{FTG},\ l_L(G,\delta)=(G,l_L(\delta))$$

$$\forall f\in \mathrm{hom}_{\mathbf{FTG}}((G_1,\delta_1),(G_2,\delta_2)),\ l_L(f)=f_c$$

则 l_L 是一函子。

由定理 6.5.1 及命题 6.5.2 容易证得以下定理。

定理 6.5.3 l_L 是ω_L 的右伴随。

证 只需证 $\forall(G,\tau)\in \mathrm{ob}\,\mathbf{TG}$，$\forall(G_1,\delta_1)\in\mathbf{FTG}$，$\forall f\in \mathrm{hom}_{\mathbf{TG}}((G,\tau),(G_1,l_L(\delta_1)))$，存在惟一的 $f_*\in \mathrm{hom}_{\mathbf{FTG}}((G,\omega_L(\tau)),(G_1,\delta_1))$，使下图(图 6-14) 可换。

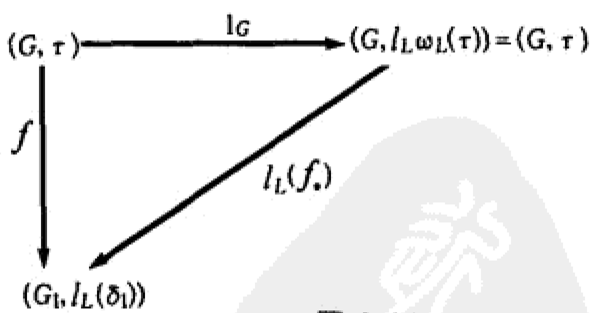


图 6-14

令 f_* 是由分明映射 f 诱导的LF 映射，则

$$f_*\in \mathrm{hom}_{\mathbf{FTG}}((G,\omega_L(\tau)),(G_1,\delta_1))$$

事实上，$\forall A\in\delta_1$，$\forall r\in P(L)$，因

$$l_r(f_*^{-1}(A))=f^{-1}(l_r(A))\in\tau$$

故 $f_*^{-1}(A) \in \omega_L(\tau)$，所以 f_* 连续，又，$l_L(f_*) = f$，因此 $l_L(f_*)1_G = f$，即图形(图 6-14)可换，而 f_* 的惟一性是显然的。

由定义 6.5.4 和定理 6.5.2 立得以下定理。

定理 6.5.4 TG 是 FTG 的余反射子范畴。

下面转向对另一函子 μ 的讨论。

我们已经知道 **FITG** 是 **FTG** 的满子范畴，现用 μ:**FITG** → **FTG** 表示嵌入函子来构造它的右伴随。

定义 6.5.5 设 (G,δ) 是 LF 拓扑空间，称 $\zeta(\delta) = \omega_L l_L(\delta)$ 为 δ 的诱导化。

可以直接推出以下命题。

命题 6.5.3 对 LF 拓扑空间 (G,δ)，$\zeta(\delta) \geqslant \delta$，且 $\zeta(\delta) = \delta$ 当且仅当 δ 是诱导的。

由上面的定理可得以下定理。

定理 6.5.5 令 ζ:**FTG** → **FITG**

$$\forall (G,\delta) \in \text{ob}\,\mathbf{FTG}, \zeta(G,\delta) = (G,\zeta(\delta))$$

$$\forall f \in \hom_{\mathbf{FTG}}((G_1,\delta_1),(G_2,\delta_2)), \zeta(f) = \omega_L l_L(f)$$

则 ζ 是一函子。

定理 6.5.6 ζ 是 μ 的右伴随。

证 只需证 $\forall (G,\delta) \in \text{ob}\,\mathbf{FITG}$，$\forall (G_1,\delta_1) \in \text{ob}\,\mathbf{FTG}$，$\forall f \in \hom_{\mathbf{FITG}}((G,\delta),(G_1,\zeta(\delta_1)))$，存在惟一的 $f_* \in \hom_{\mathbf{FTG}}((G,\delta),(G_1,\delta_1))$，使下面的图形(图 6-15)可换。

令 $f_* = f$，则由

$$\delta_1 \leqslant \omega_L l_L(\delta_1) = \zeta(\delta_1)$$

知 f_* 是 LF 连续映射，故

$$f_* \in \hom_{\mathbf{FTG}}((G,\delta),(G_1,\delta_1))$$

f_* 的惟一性是显然的。

下证 $\zeta(f_*) = f$。

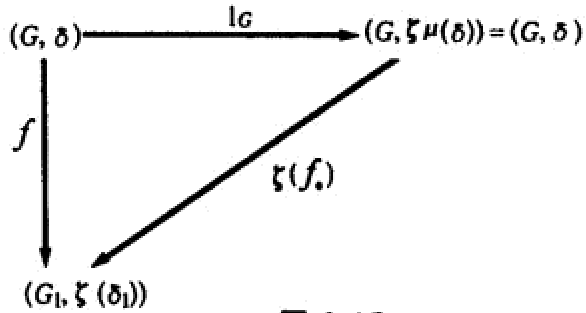


图 6-15

由 $f_*:(G,\delta)\to(G_1,\delta_1)$,有

$$l_L(f_*):(G,l_L(\delta))\to(G_1,l_L(\delta_1))$$

进而

$$\omega_L l_L(f_*):(G,\omega_L l_L(\delta))\to(G_1,\omega_L l_L(\delta_1))$$

但

$$\delta=\omega_L l_L(\delta)$$
$$\omega_L l_L(\delta_1)=\zeta(\delta_1)$$
$$\omega_L l_L(f_*)=\zeta(f_*)$$

因此

$$\zeta(f_*):(G,\delta)\to(G_1,\zeta(\delta_1))$$

所以 $\zeta(f_*)=f$。

推论 1 **FITG** 是 **FTG** 的余反射子范畴。

我们再讨论遗忘函子 ϵ。

定义 6.5.6 令 $\epsilon:\mathbf{FTG}\to\mathbf{Grp}$

$$\forall(G,\delta)\in \text{ob}\,\mathbf{FTG},\epsilon(G,\delta)=G$$

$$\forall f\in \hom_{\mathbf{FTG}}((G_1,\delta_1),(G_2,\delta_2)),\epsilon(f)=f_c$$

则称 ϵ 是一遗忘(LF 拓扑结构的)函子。

首先构造 ϵ 的左伴随,下面的命题是显然的。

命题 6.5.4 设 $G\in \text{ob}\,\mathbf{Grp}$,则$(G,\delta_{\max})\in \text{ob}\,\mathbf{FTG}$,这里 $\delta_{\max}$ 是 G 上的 LF 离散拓扑。

由此命题不难证得以下定理。

定理 6.5.7 令 $\varepsilon_l: \mathbf{Grp} \to \mathbf{FTG}$

$$\forall G \in \text{ob}\ \mathbf{Grp}, \varepsilon_l(G) = (G, \delta_{\max})$$

$$\forall f_c \in \hom_{\mathbf{Grp}}(G_1, G_2), \varepsilon_l(f_c) = f$$

这里 $f:(G_1, \delta_{1\max}) \to (G_2, \delta_{2\max})$ 是由 f_c 诱导的 LF 映射，则 ε_l 是一函子。

定理 6.5.8 ε_l 是 ε 的左伴随。

证 只需证明 $\forall G \in \text{ob}\ \mathbf{Grp}, \forall (G_1, \delta) \in \text{ob}\ \mathbf{FTG}, \forall f \in \hom_{\mathbf{Grp}}(G, G_1)$，存在惟一的 f_* 是由分明映射 f 诱导的 LF 映射，则 $f_*:(G, \delta_{\max}) \to (G_1, \delta_1)$ 显然连续，故 $f_* \in \hom_{\mathbf{FTG}}((G, \delta_{\max}), (G_1, \delta_1))$，$f_*$ 的惟一性是显然的。至于 $\varepsilon(f_*)1_G = f$，则更是明显的。

同理可以构造 ε 的右伴随(见图 6-16)。

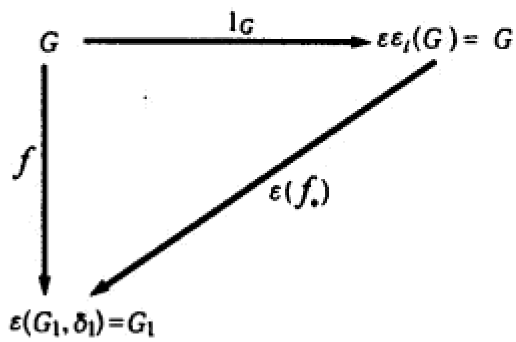


图 6-16

ISBN 7-5632-1534-4

9 787563 215348 >

ISBN 7-5632-1534-4
O · 89 定价：25.00元